Universidade Católica Portuguesa
Faculdade de Engenharia

Classificação Taxonómica dos Ataques de Engenharia Social

Caracterização da Problemática da Segurança de Informação

em Portugal relativamente à Engenharia Social

Francisco José Albino Faria Castro e Silva

Dissertação para a obtenção do Grau de Mestre em Segurança dos Sistemas de Informação

Júri

Prof. Doutor Rui Jorge Correia Mendes Alves Pires (Presidente)
Prof. Doutor César Augusto dos Santos Silva
Prof. Doutor Tito Lívio dos Santos Silva (Orientador)

Maio 2013

RESUMO

Nos nossos dias, a informação é um recurso de vital importância. Com a necessidade de protegerem esse activo, as empresas implementam mecanismos com o objectivo de garantirem a integridade, confidencialidade e a disponibilidade da informação. Na dificuldade em ultrapassarem as barreiras tecnológicas de segurança, os ataques têm sido incrementalmente direccionados ao elemento humano – o utilizador, principalmente, pese embora técnicos possam também ser o alvo destes. Os atacantes, através da aplicação de técnicas e da exploração das vulnerabilidades do ser humano, entre as quais a ingenuidade, a curiosidade e a confiança, concretizam os seus objectivos.

Deste modo, e tendo em conta a relevância do problema, surge este trabalho que tem como objectivo:

- identificar o nível de conhecimento dos utilizadores e dos responsáveis de TI em relação à problemática da engenharia social em Portugal,
- identificar as medidas de segurança adoptadas,
- identificar as técnicas mais usadas,
- identificar o principal objectivo dos ataques,
- identificar a preocupação com a formação,
- Apresentar uma nova classificação dos ataques de engenharia social.

A investigação envolveu 393 utilizadores que frequentam as redes sociais e 41 responsáveis por sistemas de informação. Tendo em vista a prossecução dos objectivos analisaram-se as respostas aos questionários. A análise dos dados revelou:

- que o nível de conhecimento sobre a problemática da engenharia social é reduzido;
- em relação às medidas de segurança, verifica-se que a instalação do antivírus e a utilização de uma firewall são as mais aplicadas.
- em relação às técnicas de ataque constatou-se que o Phishing e o Spam-mail são as mais usadas;
- que a principal motivação dos ataques é o roubo de informação.
- a preocupação com a formação dos colaboradores não é uma prioridade, entre as empresas inquiridas, apenas 23% promovem acções de formação.

Com o objectivo de auxiliarmos os responsáveis de segurança no desenvolvimento de políticas e controlos, foi proposta uma nova forma de abordar os ataques de engenharia social, através da classificação dos ataques com base no tipo de abordagem, entre a vítima e o atacante, directa ou indirecta. Na abordagem directa não existe a necessidade de utilização de qualquer meio de

comunicação, o contacto é presencial. A abordagem indirecta é realizada através da utilização dos meios de comunicação. Na proposta realizada, as técnicas de ataque foram analisadas com base na relação de dependência entre as diversas técnicas e na identificação da relação entre as técnicas e as ameaças.

Palavras chave: Engenharia Social, Classificação dos ataques de engenharia social, Políticas de Segurança, Segurança de Informação.

ABSTRACT

Nowadays, information is a resource of vital importance. With the need to protect that asset, companies implement mechanisms aimed at ensuring the integrity, confidentiality and information availability. Due to the difficulty of overcoming the technological barriers of security, the attacks have been directed to the human element. The attackers, by applying attack techniques and exploiting human vulnerabilities, among which ingenuity, curiosity and confidence, achieve their objectives.

Thus, taking into account the relevance of the problem, this work aims to:

- identify the level of knowledge of users and IT managers concerning the problem of social engineering in Portugal,
- as well as the security measures,
- the mostly used techniques,
- the main aim of the attacks,
- concern about training,
- and finally present a new classification of social engineering attacks.

The research involved 393 users who use social networks and 41 information system managers. In order to achieve the objective, the answers to the questionnaires were analysed. Data analysis revealed that:

- the level of knowledge about the problem of social engineering is low,
- regarding security measures, it appears that antivirus installation and use of a firewall are the most applied,
- regarding the attack techniques we found that Phishing and spam-email are the most used,
- and that the main motive of the attacks is the theft of information,
- the concern with employee training is not a priority among the companies surveyed, with only 23% promoting training workshops.

In order to support the security managers in the development of security policies, we propose a new way of approaching social engineering attacks through the classification of attacks based on the type of approach, between the victim and attacker, direct or indirect. In the direct approach there is no need to use any means of communication, the contact is in person. The indirect approach is accomplished through the use of communication media. In this study, the

attack techniques were analysed based on the interdependence between the various techniques, and on the identification of the relationship between techniques and threats.

Keywords: Social Engineering, Classification of social engineering attacks, security policies, Information Security.

À memória dos

meus avós,

Tio e Irmã…

AGRADECIMENTOS

Para a realização desta investigação foram vários os intervenientes que colaboraram directa e indirectamente, os quais merecem o meu reconhecimento e gratidão.

Aos meus orientadores, Professor Doutor Tito Santos Silva e o Dr. João Barreto, por todo o apoio, incentivo, compreensão e disponibilidade com que acompanharam este trabalho, assim como pelos comentários e sugestões.

À Faculdade de Engenharia da Universidade Católica Portuguesa, que viabilizou e tornou possível a realização deste Mestrado.

À minha filha, aos meus pais e amigos por todo o apoio, incentivo e motivação que proporcionaram.

A todos os meus sinceros agradecimentos

Índice

RESUMO 1

ABSTRACT 3

AGRADECIMENTOS 6

ÍNDICE DE FIGURAS 9

ÍNDICE DE GRÁFICOS 10

ÍNDICE DE QUADROS 14

ÍNDICE DE TABELAS 14

GLOSSÁRIO 15

CAPITULO I – INTRODUÇÃO TEÓRICA 16

1.1. ENGENHARIA SOCIAL 16

1.2. AS PRINCIPAIS FALHAS HUMANAS 18

1.2.1. OS FACTORES DE INFLUÊNCIA 18

1.2.2. OS FACTORES DE ATAQUE 21

1.3. CICLO DE DESENVOLVIMENTO DE UM ATAQUE DE ENGENHARIA SOCIAL. 22

1.4. DEFINIÇÃO DAS TÉCNICAS DE ENGENHARIA SOCIAL 23

1.4.1. IMPERSONATION/PRETEXTING 23

1.4.2. DUMPSTER DIVING/TRASHING 23

1.4.3. SPYING AND EAVESDROPPING 24

1.4.4. SHOULDER SURFING 24

1.4.5. HOAXING 25

1.4.6. TAILGATING 25

1.4.7. BAITING 26

1.4.8. MENSAGENS NÃO SOLICITADAS 26

1.4.8.1. POP-UPS 26

1.4.8.2. SPAM-MAIL 27

1.4.8.3. PHISHING 27

1.4.8.4. SMISHING 28

1.4.8.5. VISHING 28

1.4.9. MALWARE / INTERESTING SOFTWARE 29

1.4.10. PHARMING 29

1.4.11. FOOTPRINTING 30

1.4.12. ENGENHARIA SOCIAL INVERSA 30

1.5. IDENTIFICAÇÃO DO PROBLEMA EM ESTUDO 31

1.6. ESTADO DA ARTE 32

1.7. OBJECTIVO DA DISSERTAÇÃO 37

1.7.1. Objectivo geral 37

CAPÍTULO II – METODOLOGIA 39

2.1. Caracterização do estudo 39

2.2. Selecção da amostra 43

2.3. Instrumentos utilizados 44

2.4. Procedimento 46

2.5. Análise dos dados 48

CAPÍTULO III – RESULTADOS E DISCUSSÃO 49

3.1. Análise dos resultados do questionário aplicado aos responsáveis TI. 49

3.1.1. Identificação dos principais serviços utilizados. 51

3.1.2. As medidas de segurança aplicadas 53

3.1.3. O nível de conhecimento sobre a engenharia social 56

3.1.4. As técnicas de ataque mais utilizadas. 57

3.1.5. Os principais alvos de ataques de engenharia social 59

3.1.6. A principal motivação dos ataques 59

3.1.7. Participação dos ataques 60

3.1.8. A abordagem de segurança 60

3.1.9. Formação dos colaboradores 61

3.1.10. O sentimento em relação aos riscos de segurança no futuro 61

3.2. Análise dos resultados do questionário aplicado aos utilizadores. 63

3.2.1. Caracterização dos inquiridos 63

3.2.2. Caracterização dos inquiridos que indicaram o email, quanto ao género e à faixa etária 64

3.2.3. Identificação dos principais serviços utilizados. 65

3.2.4. As preocupações com segurança na utilização do telefone e da internet. 68

3.2.5. As medidas de segurança aplicadas 68

3.2.6. O nível de conhecimento sobre a engenharia social 71

3.2.7. As técnicas de ataque mais utilizadas. 73

3.2.8. A principal motivação dos ataques 75

3.2.9. A participação dos ataques 75

3.2.10. Identificação das plataformas de ataque. 75

3.2.11. O sentimento em relação aos riscos de segurança no futuro. 76

CAPÍTULO IV – DEFINIÇÃO DE UMA TAXONOMIA DE BASE 78

4.1. Introdução 78

4.2. Definição da Taxonomia de Base 79

4.2.1. Identificação da relação entre as técnicas e as ameaças. 88

4.3. VALIDAÇÃO DA PROPOSTA APRESENTADA 88
4.4. CONTRIBUIÇÃO DA TAXONOMIA PROPOSTA 96
CAPÍTULO V – CONCLUSÕES 97
5.1. DISCUSSÃO 97
5.2. TRABALHO FUTURO 101
BIBLIOGRAFIA 102
ANEXOS 108
ANEXO I – INQUÉRITO AOS RESPONSÁVEIS TI 109
ANEXO II – INQUÉRITO AOS UTILIZADORES 114
ANEXO III - TABELAS COM OS CÁLCULOS DAS MARGENS DE ERRO 119

Índice de Figuras

Figura 1.1. Classificação dos Ataques de Engenharia Social (Peltier, 2006) 32
Figura 1.2. Classificação dos Ataques de Engenharia Social, (Twitchell, D. P, 2006) 33
Figura 1.3. Classificação dos Ataques de Engenharia Social, (Sandouka, Cullen, & Mann, 2009) 34
Figura 1.4. Classificação dos Ataques de Engenharia Social, (Janczewski, L. J.; Lingyan, F., 2010) 34
Figura 1.5.Classificação dos Ataques de Engenharia Social, (Foozy, Ahmad, Abdollah, Yusof, & Zaki, 2011) 35
Figura 6. Cálculo do IC para μ com grau de confiança 1-α (Jordán, Gladys Castillo, 2008) 48
Figura 7. Classificação proposta dos ataques de engenharia social. 79

Índice de Gráficos

Gráfico 3.1.Descrição das empresas que responderam ao inquérito de acordo com sector de actividade 49

Gráfico 3.2. Identificação da formação 50

Gráfico 3.3. Descrição das actividades do sector terciário 50

Gráfico 3.4.Resultado das respostas, quando questionados sobre quais os serviços que utilizam, com intervalo de confiança de 95%. As margens de erro estão indicadas para cada serviço apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 1) .. 51

Gráfico 3.5. Resultado das respostas quando questionados sobre quais as medidas de segurança adoptadas, com intervalo de confiança de 95%. As margens de erro estão indicadas para cada serviço apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 2) 54

Gráfico 3.6. Resultado das respostas quando questionados: " Se já ouviram falar em ataques de engenharia social", com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 3) 56

Gráfico 3.7. Resultado das respostas quando questionados: "Assinale os ataques de que já ouviu falar?", com intervalo de confiança de 95%. As margens de erro estão indicadas para cada técnica de ataque apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 4) 57

Gráfico 3.8. Resultados das respostas quando questionados: "Se já sofreram algum tipo de ataque de engenharia social?", com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 5) 58

Gráfico 3.9. Resultado das respostas quando questionados para identificar o tipo de ataque de que foram alvo, com intervalo de confiança de 95%. As

margens de erro estão indicadas para cada técnica de ataque apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 6) 58
Gráfico 3.10. Resultado das respostas quando questionados para identificarem, entre os colaboradores, os principais alvos de ataques de engenharia social, com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 7) 59
Gráfico 3.11. Resultado das respostas quando questionados para identificar o principal objectivo do ataque, com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 8) 59
Gráfico 3.12. Resultado das respostas quando questionados se após sofrerem um ataque efectuaram alguma participação a alguma autoridade, com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 9) 60
Gráfico 3.13. Resultado das repostas quando questionados sobre qual a abordagem aplicada depois do ataque, com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 10) 60
Gráfico 3.14. Resultado das respostas dadas quando questionados se promovem acções de formação dos colaboradores sobre os ataques de engenharia social, com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 11) 61
Gráfico 3.15. Resultado das respostas dadas quando questionados sobre qual o sentimento em relação aos riscos de segurança no futuro, com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 12) 61

Gráfico 3.16. Resultado das respostas dadas quando questionados para identificarem no futuro quais serão as plataformas mais utilizadas nos ataques de engenharia social, com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 13) 62
Gráfico 3.17.Caracterização da amostra em termos de género. 63
Gráfico 3.18. Caracterização da amostra com base no género e na faixa etária 63
Gráfico 3.19. Caracterização dos inquiridos que indicaram o email com base no género, com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 14) 65
Gráfico 3.20. Caracterização dos inquiridos que indicaram o email com base na idade, com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 15) 65
Gráfico 3.21. Respostas obtidas quando questionados quais os serviços que utilizam, com intervalo de confiança de 95%. As margens de erro estão indicadas para cada serviço apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 16) 66
Gráfico 3.22. Resultado das respostas dadas quando questionados se quando realizam operações através do telefone/internet se preocupam com a segurança, com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 17) 68
Gráfico 3.23. respostas obtidas com base na faixa etária, quando questionados sobre quais os cuidados que adoptam quando navegam na internet, com intervalo de confiança de 95%. As margens de erro estão indicadas para cada medida apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 18) 69
Gráfico 3.24.Resultado das respostas dadas quando questionados para indicar qual a proveniência do antivírus que têm instalado no computador, com intervalo de confiança de 95%. As margens de erro estão indicadas

apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 19) 70
Gráfico 3.25. Resultado das respostas quando questionados se já ouviram falar em ataques de engenharia social, com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 20) 71
Gráfico 3.26. Resultado das respostas, de acordo com a faixa etária, sobre as técnicas de ataque mais conhecidas, com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 21) 72
Gráfico 3.27. Resultados das respostas quando questionados se foram alvo de alvo de um ataque de engenharia social, com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 22) 73
Gráfico 3.28. Resultados das respostas quando questionados se o ataque de que foram alvo foi bem sucedido, com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 23) 73
Gráfico 3.29. Resultado das respostas quando questionados para identificar o tipo de ataque de que foram alvo, com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 24) 74
Gráfico 3.30. Resultado das respostas quando questionados para identificar qual o motivo do ataque, com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 25) 75
Gráfico 3.31. Resultado das respostas quando questionados para identificarem a entidade onde participaram o ataque de que foram alvo, com intervalo de

confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 26) 75
Gráfico 3.32. Resultado das respostas quando questionados para identificar qual a plataforma de ataque usada, com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 27) 76
Gráfico 3.33. Resultado das respostas quando questionados para identificar no futuro quais serão as plataformas de ataque mais utilizadas, com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 28) 76
Gráfico 3.34. Resultado das respostas quando questionados para identificarem qual o sentimento em relação aos riscos de segurança no futuro, com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 29) 77

Índice de Quadros

Quadro 4.1. Identificação da relação entre as técnicas. 84
Quadro 4.2 Validação das relações entre as técnicas. 84
Quadro 4.3. Identificação da relação entre as técnicas e as ameaças 88

Índice de Tabelas

Tabela 2.1. Formulação do questionário aos responsáveis de TIs. 39
Tabela 2.2. Formulação do questionário dos utilizadores 41
Tabela 2.3. Caracterização dos elementos da amostra com base no género e na faixa etária dos utilizadores 44

GLOSSÁRIO

DoS - negação de serviço

Consiste num ataque a um sistema ou rede que tem como objectivo impedir aos utilizadores o acesso a um determinado serviço.

Endereço IP

O endereço IP é uma sequência de números composta de 32 bits, que permite identificar um determinado equipamento na rede local ou pública.

Engenheiro social ou atacante

Pessoa que através da utilização de um conjunto de técnicas de engenharia social executa um ataque.

Firewall

Pode ser definido como uma barreira de segurança que controla o tráfego de dados impedindo tráfego não autorizado.

peer-to-peer (P2P)

Uma rede Peer-to-Peer (P2P) consiste num conjunto de computadores que comunicam entre si de forma descentralizada. Os computadores podem, simultâneamente, ser clientes e servidores.

Políticas de Segurança

Consistem num conjunto formal de regras que definem as atitudes, os procedimentos e os mecanismos de segurança que devem ser implementados.

Técnicas de Ataques de engenharia social

As técnicas de engenharia social são consideradas como um meio para um fim e não necessariamente um ataque.

CAPITULO I – INTRODUÇÃO TEÓRICA

Neste capítulo será desenvolvida uma análise introdutória sobre a engenharia social e de toda a problemática que lhe está associada. Serão identificadas as principais falhas humanas exploradas pelos engenheiros sociais no desenvolvimento de um ataque e, de seguida, descritas as principais técnicas de ataque de engenharia social. Por fim será feita a identificação do problema em estudo, do estado da arte e dos objectivos da investigação.

1.1. ENGENHARIA SOCIAL

A informação é um recurso precioso nas organizações, eventualmente o mais importante (seguramente é-o numa miríade de actividades). Numa sociedade globalizada, a boa gestão da informação contribui para a competitividade da pessoa e da organização. Como um recurso importante necessita de ser protegido.

> " *Information is an asset which, like other important business assets, has value to an organization and consequently needs to be suitably protected.*" (BS ISO/IEC 27002, 2005).

Com a evolução das tecnologias as organizações tem investido parte dos seus recursos na modernização dos Sistemas de Informação. Todo esse investimento tem sido dirigido na aquisição de sistemas mais modernos e seguros, dado o valor da informação, relegando amiúde o factor humano para um papel secundário. Tal degenerou, logica e consequentemente, na orientação dos ataques para a exploração das vulnerabilidades do ser humano e obtenção posterior de informação – a Engenharia Social.

> "*Social engineering is generally a hacker's clever manipulation of the natural human tendency to trust.*" (Granger S. , Social Engineering Fundamentals, Part I: Hacker Tactics, 2001).

Actualmente, a Engenharia Social é um dos maiores riscos de segurança das pessoas e organizações. As técnicas de ataque são cada vez mais sofisticadas, aproveitam-se da inocência dos utilizadores, que na sua maioria não se apercebem do ataque, para a concretização dos seus objectivos: obtenção de informação não autorizada.

Ao contrário dos métodos tradicionais de ataque, onde o "atacante" é um especialista técnico, na engenharia social o atacante necessita apenas de utilizar as suas habilidades sociais na realização de um ataque.

Ao efectuarmos pesquisas sobre o tema, encontramos interpretações diferenciadas em campos de conhecimento distintos. Engenharia Social é um termo utilizado pela ciência política desde o início do século XX que consistia na utilização de métodos inteligentes para a resolução dos problemas sociais.

Muitas são as interpretações e definições na literatura para o termo. A essência comum entre todas as interpretações é que a engenharia social envolve métodos que pretendem controlar o comportamento humano como um meio para a concretização de um objectivo. O objectivo do ataque muitas vezes só é atingido depois da aplicação de um conjunto de várias técnicas.

O "engenheiro social" utiliza a psicologia humana para explorar os sentimentos e as emoções de forma a controlar o comportamento da vítima.

A detecção dos ataques de engenharia social não é um processo fácil (Tiantian, 2007). Apesar da existência de ferramentas e de linhas de orientação com o objectivo de reduzir o risco, é um tipo de ataque que está em constante evolução e tem vindo a aumentar nos últimos tempos (Abraham & Chengalur, 2010) .

A falta de consciência dos utilizadores em relação aos perigos, a falta de conhecimento das técnicas de engenharia e o excesso de autoconfiança de muitos utilizadores são os elementos que promovem o sucesso da engenharia social.

As organizações debatem-se hoje com o problema de garantir a segurança da sua informação. A Segurança da Informação, segundo BS ISO/IEC *27002* , é garantida pela preservação de três factores: Confidencialidade - garantia de que a informação é acessível apenas pelas pessoas autorizadas; Integridade - garantia de que a informação não sofreu alterações provocadas por pessoas não autorizadas e Disponibilidade - a garantia de que os utilizadores autorizados têm acesso à informação sempre que necessitem (ISO, 2005).

É necessário que os utilizadores tenham a consciência do valor da informação e de que as suas acções podem influenciar directa ou indirectamente a segurança da informação. O primeiro passo necessário para garantir a segurança da informação deve passar pela consciencialização dos utilizadores.

> " *A segurança compreende três componentes – pessoas, processos e tecnologia – e o resultado final deve ser a preservação da confiança*" (Mccartthy & Campbell, 2003).

A formação dos utilizadores é um passo importante pois irá permitir uma melhor implementação das políticas de segurança. A implementação das medidas de segurança poderá ser realizada através do desenvolvimento de programas de sensibilização. Estes programas poderão ser usados para garantir que as políticas de segurança e as melhores práticas sejam implementadas e cumpridas. As políticas de segurança são um elemento fundamental e estratégico para implementar a segurança (Lafrance, 2004).

> "*Organizations should develop clear, concise security policies that are enforced consistently throughout the organization; develop simple rules defining what information is sensitive and develop a data classification policy and require the requestors identity when restricted actions are required* " (Peltier, 2006)

Um utilizador bem informado com muito menos probabilidade será vítima de um ataque que os demais. Complementarmente, os utilizadores devem fazer parte das práticas de segurança não só como observadores mas também como elementos intervenientes, pois eles são o elo mais "fraco".

> " *Geralmente as pessoas são o ponto mais susceptível num esquema de segurança. Um trabalhador maldoso, negligente ou alheio à política de informação de uma organização pode comprometer até a melhor segurança*" (Commer, 1998).

1.2. AS PRINCIPAIS FALHAS HUMANAS

1.2.1 Os Factores de Influência

Cialdini (2001) no seu livro "*Influence: The Psychology of Persuasion"* descreve as caracteristicas humanas que são exploradas num ataque de engenharia social: Retribuição; Compromisso/Consistência; Prova Social; Simpatia; Autoridade e a Escassez.

1.2.1.1 Retribuição (Reciprocation)

O ser humano, por natureza e educação, sente necessidade de retribuir um favor ou uma oferta que lhe tenha sido feita. (Cialdini, 2001) Quando alguém nos fornece um bem ou serviço, sentimos uma obrigação ou um sentimento de dívida para com a pessoa que nos prestou esse gesto. Essa retribuição poderá ser feita por diversas formas. Esta regra muitas vezes é explorada, pelo engenheiro social, devido à força que tem sobre as pessoas. Pode resultar em trocas desiguais de favores ou informações. No decurso do pagamento da dívida, a pessoa paga (monetariamente ou por acções) mais do que é devido para aliviar o seu sentimento de culpa (Cialdini, 2001).

1.2.1.2 Compromisso, Consistência (Commitment and Consistency)

O compromisso e a consistência são duas condições do ser humano susceptíveis de serem usadas num ataque de engenharia social. O principio sugere, uma vez tomada a decisão, que a pessoa sente-se responsável em se comportar de forma consistente com a decisão tomada. Nos nossos dias as pessoas são valorizadas pelo cumprimento dos seus compromissos e pela consistência das suas posições. A nossa inclinação para agir de forma consistente, por vezes de forma mecanizada, na maioria das situações do dia-a-dia torna-nos suscpetíveis de tomar uma decisão ou atitude irreflectida (Cialdini, 2001).

1.2.1.3 Prova Social (Social Proof)

O princípio da prova social é uma condição que pode ser usada como uma forma eficaz de influência. O princípio da prova social é mais eficaz e influente em duas condições específicas (Cialdini, 2001):

- o primeiro é na incerteza, quando nos encontramos num estado de incerteza somos mais propensos a olhar para o comportamento dos outros para descobrir o que fazer;
- a segunda é na semelhança. As pessoas são mais propensas a seguir o comportamento dos outros com quem se identificam.
- outra característica importante do princípio da prova social é que ela funciona melhor quando a prova é apresentada pelas acções de muitas pessoas.

1.2.1.4 Simpatia (Friendliness)

As pessoas tendem a ser mais sensíveis com as pessoas de quem são amigas ou de quem gostam. Os investigadores descobriram que a atractividade, similaridade ou um simples louvor

são factores que poderão influenciar a relação de amizade entre as pessoas. Segundo Cialdini (2001), a familiaridade com alguém e a descoberta de semelhanças entre ambas são factores que levam as pessoas a gostar uma da outra. Quanto mais à vontade e amigável a vítima for com o atacante maior é a probabilidade de fornecer a informação que o atacante pretende (Cialdini, 2001).

1.2.1.5 Autoridade (Authority)

Quando alguém demonstra um determinado estatuto pela utilização de títulos (director, presidente), dinheiro, determinado tipo de carro ou vestuário, as pessoas tendem a associar essas demonstrações como pistas para a identificação do estatuto que ocupam. Por natureza o ser humano tende a responder afirmativamente aos pedidos ou às ordens de uma figura autoritária por medo de repreensão ou pela esperança de uma recompensa (Cialdini, 2001).

O engenheiro social tende a explorar esta condição, por exemplo, como uma forma de obter o acesso ao espaço ou à informação que pretende.

1.2.1.6 Escassez (Scarcity)

> *"... as pessoas atribuem mais valor para as oportunidades quando elas estão menos disponíveis .... O princípio da escassez prende por duas razões. Em primeiro lugar, porque as coisas que são difíceis de atingir são tipicamente mais valiosas .... Em segundo lugar, as coisas quando se tornam menos acessíveis, perdemos liberdades* " (Cialdini, 2001).

Um exemplo evidente de como o princípio funciona é ver como um cliente reage quando é informado ou toma o conhecimento de que um determinado produto de interesse está limitado ao stock ou em fim de stock. Por natureza o cliente compra o produto com medo de não o poder vir a ter. O termo "número limitado" é uma táctica muito eficaz e é usado diariamente pelo marketing.

Um engenheiro social poderá utilizar esta condição na realização de um ataque. Por exemplo, desenvolvendo uma página web propõe a venda de um produto em fim de vida em conjunto com ofertas. A vítima atraída pelas ofertas e por pensar ser uma das poucas pessoas que irá possuir um item tão raro, compra o item, enviando ao atacante os seus dados pessoais. Ao efectuar a "compra-falsa" e sem se aperceber, forneceu informação confidencial.

1.2.2 Os factores de Ataque

Charles Lively, baseando nas seis condições humanas descritas por Cialdini (2001) anuncia os seguintes como vectores de ataque explorados e utilizados pelos engenheiros sociais: Descuido; Zona de Conforto; Ser Útil e o Medo (Lively Jr, 2004).

1.2.2.1 Descuido (Carelessness)

O descuido é uma das principais falhas responsável pelo incumprimento das medidas de segurança. A vítima acaba por ser vítima do seu acto. Esta falha pode ser explorada pelo atacante para a obtenção de informação confidencial. O descuido auxilia o engenheiro social principalmente na fase de planeamento do ataque.

> "*A falta de cuidado, muitas vezes é a primeira fase de um ataque mais complexo"* (Lively Jr, 2004).

1.2.2.2 Zona de Conforto (Confort Zone)

O ser humano quando está numa zona de conforto, encontra-se num estado mais relaxado, confortável, o que torna o seu desempenho mais limitado tendo por consequência o incumprimento das normas de segurança. Esse estado promove uma sensação de segurança, reduzindo a capacidade de percepção da ameaça pela vítima. Este estado será explorado pelo atacante para a concretização do seus objectivos. A "simpatia" e a "prova social" são as condições que tendem a ser facilmente exploradas na zona de conforto (Lively Jr, 2004).

1.2.2.3 Útil (Helpful)

O ser humano por natureza tem necessidade de sentir-se útil. O engenheiro social poderá explorar esta condição transmitindo à vítima a ideia de que necessita do seu apoio. Numa organização, o atacante poderá fazer-se passar por um novo funcionário com a necessidade de assistência, tentando dessa forma obter a informação de que necessita para atingir o objectivo ou que poderá ser útil para o desenvolvimento do ataque (Lively Jr, 2004).

1.2.2.4 Medo (Fear)

O medo é um vector susceptível de ser usado como uma arma a favor do atacante. A vítima poderá sentir-se pressionada por alguém que através da sua atitude e da forma como se

apresenta transmite a ideia de autoridade. O ser humano sob a pressão do medo reduz a sua capacidade de desempenho e de acção (Lively Jr, 2004).

Por exemplo, num ataque de engenharia social, o atacante poderá fazer com que a vítima acredite que algo de mal poderá acontecer mas que pode ser evitado se realizar o que o atacante sugere.

1.3. CICLO DE DESENVOLVIMENTO DE UM ATAQUE DE ENGENHARIA SOCIAL.

Ant Allan refere que o ciclo de desenvolvimento de um ataque de engenharia social é constituído por quatro fases: (Allan, Noakes-Fry, & Mogull, 2005)

Recolha de Informação: O atacante poderá utilizar várias fontes para obtenção da informação relativa ao seu alvo. Este processo pode passar por análise do lixo, espionagem, pesquisas na internet, redes sociais entre outros. A informação obtida nesta fase servirá de base para a fase seguinte.

Desenvolvimento da Relação: Depois de definido o objectivo do ataque, do alvo a atacar e do pretexto a utilizar, o atacante tenta desenvolver um relacionamento com a vítima de forma a criar uma relação de confiança. A duração desse relacionamento é variável.

Exploração da Relação: O atacante manipula a vítima para obtenção da informação que pretende ou informação que permita executar o seu plano. Esta fase poderá ser a final ou a preparação para a final**.**

Execução para atingir o objectivo: O resultado da fase anterior é usado para a concretização dos objectivos ou para reforçar o ataque. O objectivo final poderá ser atingido com apenas um ciclo ou poderá dar início a um outro.

1.4. DEFINIÇÃO DAS TÉCNICAS DE ENGENHARIA SOCIAL

1.4.1. Impersonation/Pretexting

Impersonation é uma das técnicas mais importantes de engenharia social. Num ataque deste tipo o atacante deve possuir informação necessária para uma melhor personificação da vítima por quem se está a fazer passar (Redmon, 2005).

Em alguns casos para uma melhor representação poderá ser necessário demonstrar um tom sério e ter em atenção as características da voz da vítima.

A tecnologia VoIP (*Voz sobre IP*) é muita usada neste tipo de ataque por ser mais difícil rastrear um endereço IP do que um número de telefone convencional.

Pretexting é uma técnica que consiste na obtenção de informação sob um falso pretexto, sendo mais do que uma simples mentira (Baer, 2008). É o acto de criar e usar um determinado cenário de forma a conseguir com que a vítima forneça a informação ou execute uma determinada acção que numa outra circunstância não faria. Na maioria das vezes, por via de pesquisa anterior, assenta na personificação de alguém com autoridade legítima como via de estabelecimento de confiança.

1.4.2. Dumpster Diving/Trashing

Dumpster Diving, também conhecido como *trashing,* é um outro método muito popular de engenharia social. Numa pesquisa ao lixo é possível encontrar uma enorme variedade e quantidade de informação: listas com extensões telefónicas, lista dos empregados, organogramas, manuais dos sistemas utilizados, memorandos, relatórios com informações estratégicas e até anotações com login e senha dos utilizadores, inventário dos equipamentos, extractos bancários, facturas, cassetes, fitas, cds, etc.

As pessoas, no seu dia-a-dia em casa ou no local de trabalho, têm a tendência de deitar no lixo diversas fontes de informação por falta de conhecimento do seu valor e dos perigos que poderá ter nas mãos de terceiros.

> Granger define *dumpster diving* como " *a arte de recolha de informação (ou pré-hacking)… é comum fazer-se a pesquisa de forma a pré-determinar o alvo e as*

melhores oportunidades de exploração" (Granger S. , Social Engineering Fundamentals, Part I: Hacker Tactics, 2001)

1.4.3. Spying and eavesdropping

Com o aumento da utilização e da importância das tecnologias de informação, os computadores, as redes locais e a Internet tornaram-se alguns dos elementos utilizados no desenvolvimento das técnicas de espionagem. Hoje um atacante não necessitará de entrar num edifício e roubar uma mala com documentos confidenciais, pois através da utilização da internet poderá obter a informação armazenada num computador localizado num outro local.

As técnicas de espionagem são muito diversificadas, geralmente inovadoras, recorrendo à utilização de meios tecnológicos e de observação directa. As câmaras de filmar, os microfones, malwares, intercepção de e-mails são exemplo de alguns dos métodos utilizados.

A técnica *Eavesdropping* – consiste na escuta não autorizada de chamadas sendo uma técnica muito eficaz na recolha de informações pessoais e confidenciais (Manjak, 2006).

Support staff – é uma técnica utilizada na espionagem, onde o engenheiro social torna-se elemento de uma equipa com o objectivo de infiltrar-se. Uma vez no local caminha livremente aproveitando as oportunidades para:

- recolher informação confidencial;
- utilizar os postos de trabalho com sessão iniciada;
- utilizar a extensão telefónica para solicitar uma informação ou acesso;
- instalar mecanismos de observação, etc.

As equipas de limpeza são o exemplo do grupo de pessoas que têm acesso amplo às instalações e circulam fora das horas de expediente (Thapar, 2007).

1.4.4. Shoulder Surfing

Shoulder Surfing é uma técnica de observação directa e eficaz de obtenção de informações porque depende apenas da proximidade física entre o atacante e a vítima, observando directamente a primeira "sobre o ombro" o que a segunda está a executar. Trata-se de uma técnica muito utilizada em espaços com várias pessoas. Esta técnica poderá ser desenvolvida

através da utilização de alguns equipamentos, tais como, binóculos ou outros dispositivos que aumentem o alcance de visão (Long, 2008).

Exemplo:
O engenheiro social observa a vítima, espreitando sobre os ombros, durante o processo de autenticação, com o objectivo de obter o código pessoal.

1.4.5. Hoaxing

Hoaxing é uma técnica que consiste em fazer as pessoas acreditarem numa mentira como sendo verdade. Tem como objectivo influenciar o comportamento ou a tomada de decisão de forma rápida com o medo das consequências que poderão advir se não o fizer. A utilização da mentira tem como objectivo fazer com que a vítima tome a decisão que vá ao encontro das pretensões do atacante (Thapar, 2007).

O desenvolvimento desta técnica é muito facilitado com boas capacidades oratórias ou textuais do atacante, tornando-se mais fácil a persuasão do público-alvo.

Exemplo:
O engenheiro social através da utilização de um discurso convincente, por exemplo desvalorizando a utilização de um determinado mecanismo de segurança consegue fazer com que o público mude a sua atitude em relação à importância da sua utilização.

1.4.6. Tailgating

A característica comum neste tipo de ataque é que o atacante constrói uma personagem e depois fabrica uma falsa história à volta da personagem tentando explorar as emoções básicas da vítima, a simpatia, a ganância e o medo (Workman, 2008).

A técnica, basicamente, consiste em seguir uma pessoa com entrada autorizada num local de acesso restrito (Long, 2008).

Funcionários menos esclarecidos poderão ser facilmente induzidos em erro. Funcionários com posições de menor relevo poderão recear impedir o acesso de altos quadros e as potenciais (indevidas) consequentes represálias.

Exemplo:

São diversas as técnicas que poderão ser utilizadas, pelo engenheiro social, para a obtenção do acesso ao local:

- utilização da conversa e da simpatia para a obtenção da confiança da vítima de forma a proporcionar-lhe o acesso,
- convencer de que se esqueceu ou perdeu o cartão,
- fingir ser um novo colega do trabalho; utilizar um cartão falso e desculpar-se com uma possível avaria do mesmo,
- fazer-se passar por alguém com autoridade etc.

1.4.7. Baiting

Este tipo de ataque assenta na curiosidade e ganância das vítimas, recorrendo ao uso de unidades médias físicas (CD-ROM, USB flash drives, disquetes, etc.) disponibilizados pelo engenheiro social às primeiras (por exemplo, deixando-as *esquecidas* num local visível. Ao introduzir a unidade infectada no posto de trabalho infecta o seu computador, e potencialmente toda a rede expondo a empresa a riscos desconhecidos (Buetler, 2009).

Esta técnica muitas vezes é aplicada em testes de penetração com o objectivo de avaliar a probabilidade do risco ocorrer.

Exemplo:

O engenheiro social deixa uma *pen-usb*, num local susceptível de ser encontrada, identificada como contendo a lista dos vencimentos dos colaboradores e dos administradores da empresa. A vítima pelo interesse sobre o conteúdo, introduz a *pen-usb* no computador infectando dessa forma o posto de trabalho e toda a rede da empresa.

1.4.8. Mensagens não solicitadas

1.4.8.1. Pop-ups

O pop-up é uma técnica que consiste no aparecimento de uma janela com uma determinada mensagem. O utilizador, por vezes, sem confirmar a sua origem, aceita-a dando autorização a execução da tarefa (Thapar, 2007).

Exemplo:

A vítima encontra-se a navegar na internet, surgindo uma janela com uma mensagem a sugerir a actualização do software. Sem confirmar a origem da mensagem, a vítima autoriza a instalação de software contaminado (*malware*).

1.4.8.2. Spam-mail

O e-mail é um meio electrónico muito utilizado nos nossos dias para comunicarmos, através do qual enviamos e recebemos mensagens. É um meio de comunicação em crescimento. Em 2013, 1,9 biliões de pessoas estarão a usar o e-mail como a principal forma de comunicação (Reardon, L, 2009). Na utilização do email são diversos os perigos que podem resultar, tais como a propagação de vírus.

O *Spam*, basicamente, é o termo usado para se referir ao correio electrónico não solicitado que geralmente é enviado em massa. Esta técnica pode ser utilizada para a propagação de vírus, sobrecarregamento das contas de e-mail e paralisação dos sistemas *DoS – Denial of Service*.

MessageLabs(2010), no seu relatório anual de segurança refere, com base nas estatísticas obtidas a partir da filtragem de spam e do bloqueio de serviços que um em cada 284 e-mails contem um *malware* (Symantec, 2010).

Exemplo:

O engenheiro social através da utilização do email, como forma de despertar o interesse da vítima envia mensagens com informação útil, links de páginas, fotografias, ficheiros em anexo. Ao abrir o link ou o ficheiro anexado fica contaminado.

1.4.8.3. Phishing

O *phishing* é um tipo de ataque em que através de um processo fraudulento permite obter informação pessoal e sensível. A técnica, basicamente, consiste no envio de um e-mail à vítima como sendo de uma entidade confiável. Nesse e-mail geralmente apresenta-se um link de uma página web fraudulenta, um "clone" da página oficial, contendo os logotipos e os conteúdos da página original. Como forma de obter informação, por vezes, existe um formulário no qual solicita-se a introdução de informação confidencial, o número da conta, número fiscal, códigos de acessos, dados do cartão matriz, dados do cartão de crédito entre outros. A vítima, na sua

ingenuidade devido ao desconhecimento ou descuido das políticas de segurança fornece a informação requerida (Lee, Choi, & Kim, 2007).

Exemplo:
A vítima recebe um e-mail, com o logotipo de uma instituição, a solicitar a actualização dos dados pessoais. A vítima, inocentemente, carrega no link para actualizar os dados. Algumas vezes o endereço do site fraudulento é muito idêntico ao endereço do site oficial. Uma vez na página fraudulenta, página idêntica à página oficial, a vítima tenta fazer o login introduzindo os seus dados pessoais que serão enviados ao atacante. Ao não conseguir efectuar o login supõe que seja uma falha da internet.

O Smishing e o Vishing são variantes do phishing.

1.4.8.4. Smishing

O Smishing é uma combinação dos termos *SMS* e *Phishing*. Este tipo de ataque é muito semelhante ao conceito do *phishing*, tendo como diferença o modo de envio da mensagem. A mensagem fraudulenta em vez de ser enviada como um e-mail, é enviada como uma mensagem SMS para o telemóvel da vítima (US-CERT, 2010).

Com o aparecimento dos *smartphones*, esta técnica tem sido amplamente utilizada, uma vez que estes equipamentos permitem o acesso às páginas web através de um link.

Exemplo:
Através do envio de uma mensagem SMS, o engenheiro social informa que para manter o serviço activo deve ligar para um determinado número. Neste exemplo é possível verificar que através de um ataque *smishing* é possível realizar um ataque *vishing*.

1.4.8.5. Vishing

O ataque é idêntico ao *phishing* e ao *SMSishing* tendo como diferença a utilização da voz como forma de comunicar (US-CERT, 2010). Esta técnica é muito aplicada através da utilização da tecnologia VoIP por ser mais difícil o seu rastreamento.

Exemplo

O engenheiro social contacta com a vítima, através de uma chamada telefónica, fazendo-se passar por representante de uma entidade confiável com o objectivo de fornecer um determinado serviço ou crédito. Para a concretização do objectivo é necessário que a vítima forneça alguma informação pessoal e confidencial.

1.4.9. Malware / Interesting Software

O Malware é um software malicioso que quando inserido num sistema tem como objectivo causar danos de forma a subvertê-lo para um outro uso sem o conhecimento dos utilizadores legítimos. É o mais eficaz dos tipos de ataques de engenharia social, devido à sua natureza difusa e persistente (Abraham & Chengalur, 2010).

O Malware representa um risco significativo para os indivíduos e para as organizações pois ameaça a integridade, disponibilidade e confidencialidade da informação. Um sistema infectado poderá permitir: acesso remoto; desactivação das medidas de segurança e o envio de dados desse sistema para um terceiro sem a permissão do utilizador.

Os *vírus*, *worms*, *trojan horses*, *backdoors*, *keystroke loggers*, *rootkits* e os *spyware* são descritos como diferentes tipos de malware.

Interesting software – é uma técnica de ataque que explora a curiosidade e a necessidade da vítima. Na necessidade de um determinado software, a vítima tenta-o obter de forma não legal, correndo o risco de estar a instalar um software falsificado ou infectado, colocando o posto de trabalho vulnerável a um ataque.

1.4.10. Pharming

Quando navegamos na internet e digitamos o endereço de uma página web, esperamos ser direccionados para o site legítimo. O Pharming é um tipo de ataque especialmente técnico que explora as vulnerabilidades da rede internet.

Exemplo:

Um utilizador introduz no browser o endereço do site que pretende, por exemplo *www.banco.pt*. O pedido efectuado passa por um servidor DNS *(Domain Name System – Sistema de Nomes de Domínios*). Este servidor mapeia o endereço *www.banco.pt* para o endereço IP, por exemplo,

220.10.10.3. No entanto, na utilização da técnica do *pharming* o ataque modifica o mapeamento do serviço DNS, redireccionando o endereço *www.banco.pt* para o IP, 230.10.10.3, associado a um site falso. Esta técnica é muito semelhante à técnica de ataque *phishing*, , pois o utilizador pensa que está a aceder ao site oficial quando está a aceder ao site malicioso (Srivastava, Tushar Vishesh ;, 2007).

1.4.11. Footprinting

O *footprinting* é uma técnica de recolha de informação. Através da utilização desta técnica é possível obter informação sobre as características da empresa no âmbito da segurança, intranet/extranet, dos recursos de acesso remoto, dos sistemas, etc. (Scambray, McClure, & Kurtz, 2001).

O início do ataque começa pelo estudo da página web da empresa, local onde poderá ser obtida diversa informação, por exemplo, localização, informação económica, contactos telefónicos, e-mails, estrutura accionista, organograma da empresa, identificação dos membros de gestão, políticas de privacidade, políticas de segurança e outros links relacionados com a empresa (Scambray, McClure, & Kurtz, 2001).

O engenheiro social com base na informação obtida vai construindo a sua base de dados com informações sobre os pontos fracos da segurança. A técnica é utilizada quando por outros métodos não foi possível obter a informação. A técnica é realizada através da utilização de softwares específicos que fazem pesquisas detalhadas.

1.4.12. Engenharia Social Inversa

Num ataque de engenharia social inversa o atacante age como um especialista ou como uma pessoa em posição de autoridade à qual a vítima pede ajuda. Este tipo de ataque é chamado de inverso porque neste caso a vítima é que inicia o contacto com o atacante. Esta abordagem exige ao engenheiro social uma extensa pesquisa e preparação, a fim de criar uma situação que faça com que a vítima seja forçada a solicitar ajuda ao atacante para resolver o problema.

O processo de ataque de engenharia social inversa é constituida por três etapas (Granger S. , Social Engineering Fundamentals, Part I: Hacker Tactics, 2001):

- **Sabotagem**: é a primeira etapa, consiste em "corromper" algo que faça com que a vítima necessite de recorrer ao atacante para o resolver.

- **Publicidade**: o engenheiro social anuncia a sua capacidade para resolver o problema.

- **Auxílio**: nesta etapa o atacante demonstra-se prestável para ajudar a vítima a resolver o problema. Com este acto consegue atingir dois objectivos, a satisfação da vítima e a sua confiança.

Este tipo de ataque é também denominado como *Quid Pro-Quo* em que o atacante fornece algum incentivo que convence a vítima a divulgar informações que de outra forma não seriam compartilhados.

Exemplo:
O engenheiro social selecciona a vítima e executa uma acção que o impossibilite de trabalhar, fazendo com que a vítima recorra da sua ajuda fornecendo-lhe a informação que pretende Depois de obtido o que pretendia resolve o problema satisfazendo a necessidade da vítima e obtendo a sua confiança e gratidão.

1.5. IDENTIFICAÇÃO DO PROBLEMA EM ESTUDO

As empresas muitas vezes apenas investem na modernização do seu parque tecnológico não considerando com a devida e merecida importância o factor humano. Os ataques de engenharia social não possuem uma fórmula nem um método definido, podendo atentar a aspectos físicos e psicológicos.

O ser humano é a maior preocupação no desenvolvimento das políticas de segurança, pois, ao contrário das máquinas, é um ser de emoções, é um ser influenciável e com capacidade de influenciar. Estas características são muito difíceis de combater.

Os ataques de engenharia social têm sido apontados como um dos maiores riscos, actuais, de segurança já que se apoiam nas falhas do ser humano. Este tema tem sido amplamente discutido em determinados sectores empresariais, instituições financeiras, administração pública entre outros, pois os riscos de perda de informação através de ataques de engenharia social podem ser muito altos e afectar os factores críticos das organizações.

Os diversos estudos desenvolvidos sobre este assunto limitam-se a abordar de forma generalizada a problemática da engenharia social. No desenvolvimento das políticas de segurança, os responsáveis encontram dificuldades em desenvolver respostas aos possíveis ataques de que poderão ser alvo, desenvolvendo apenas políticas generalistas. Entre as diversas dificuldades com que se deparam, destacam-se a falta de informação sobre quais as técnicas e plataformas de ataque mais utilizadas, quais as atitudes de segurança adoptadas pelos utilizadores e o nível de conhecimento sobre a problemática da engenharia social.

1.6. ESTADO DA ARTE

O presente estudo, pela sua inovação, apresenta algumas limitações inerentes à pouca informação que ainda existe sobre o referido tema. O tema Engenharia Social ainda é um tema muito pouco explorado. A formulação exacta da maioria das definições sobre este tema varia, sendo a característica comum que deriva de cada uma delas o facto da engenharia social envolver métodos que podem controlar o comportamento humano. Na análise do estado de arte iremos abordar algumas das propostas de classificação dos ataques de engenharia social.

Peltier (2006), divide os ataques de engenharia social em duas categorias: *ataques de base-humana* e *ataques de base-técnica.*

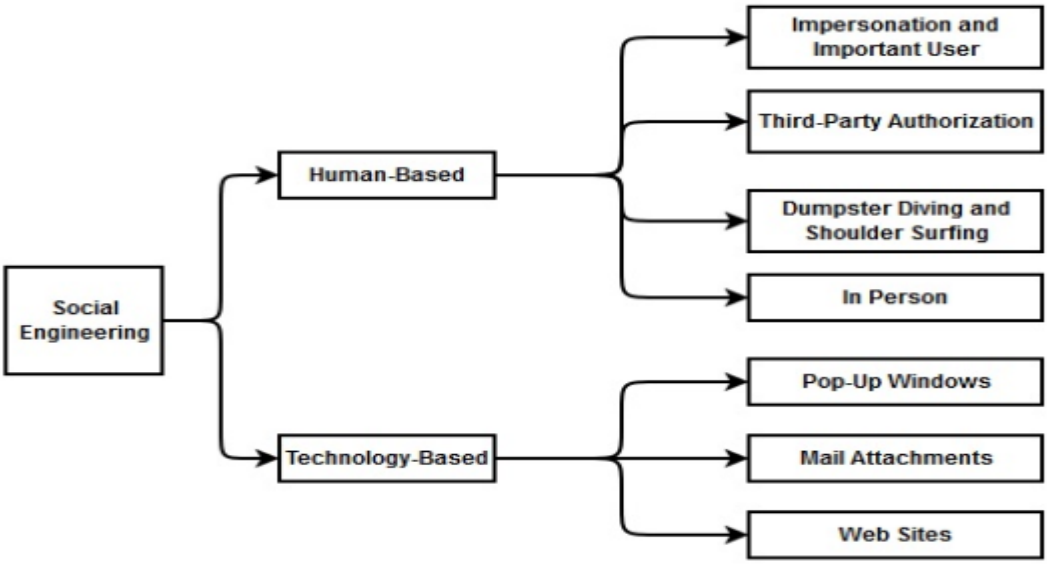

Figura 1.1. Classificação dos Ataques de Engenharia Social (Peltier, 2006)

As técnicas de *base-humana* são definidas como "*human based refers to a person-to-person interaction used to obtain the desired action*". A categoria de base-tecnológica é definida como

"*technology based means having an electronic interface to attempt to achieve the desired outcome"* (Peltier, 2006).

Peltier classifica as técnicas, o *Impersonation and Important Use, Thirdy-Party Authorization, Dumpster Diving and Shoulder Surfing e In Person* como de base-humana. Os *Pop-Up Windows, Mail attachments e Web Sites* são classificadas como ataques de base-técnica. Os ataques de base técnica, apresentadas, utilizam a Internet como meio de comunicação. É importante se referir que a técnica *In Person* é semelhante à técnica S*upport staff*.

Twitchell (2006), como é possível observar na figura 1.2, não categoriza as técnicas de engenharia social, limita-se a referenciar apenas algumas.

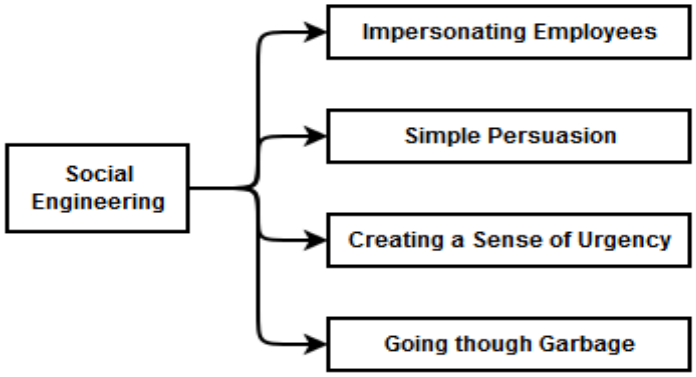

Figura 1.2. Classificação dos Ataques de Engenharia Social, (Twitchell, D. P, 2006)

Ao analisar-se a classificação proposta por Twitchell, com base na abordagem adoptada por Peltier, verifica-se que as técnicas apresentadas podem ser classificadas como técnicas de ataque de base-humana.

(Sandouka, Cullen, & Mann, 2009)na classificação proposta, na figura 1.3, também, não categorizam os ataques de engenharia social.

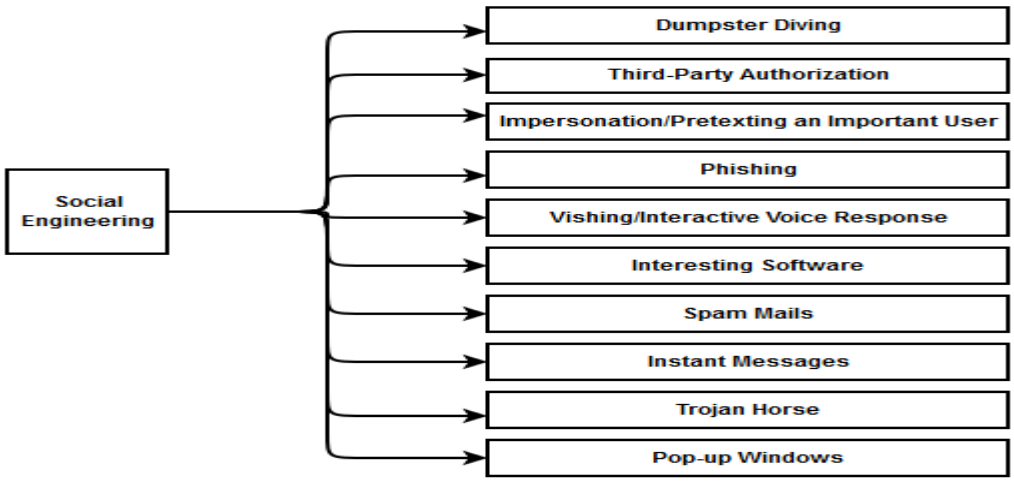

Figura 1.3. Classificação dos Ataques de Engenharia Social, (Sandouka, Cullen, & Mann, 2009)

Através da observação da figura 1.3, com base na classificação de Peltier(2006) as técnicas de ataque *Dumpster Diving*, *Third-Party Authorization; Impersonation Pretexting an Important User*, podem ser classificadas como ataques de base-humana e as restantes de base-técnica.

Janczewski & Lingyan (2010), na classificação proposta agrupam as técnicas de engenharia social em duas categorias.

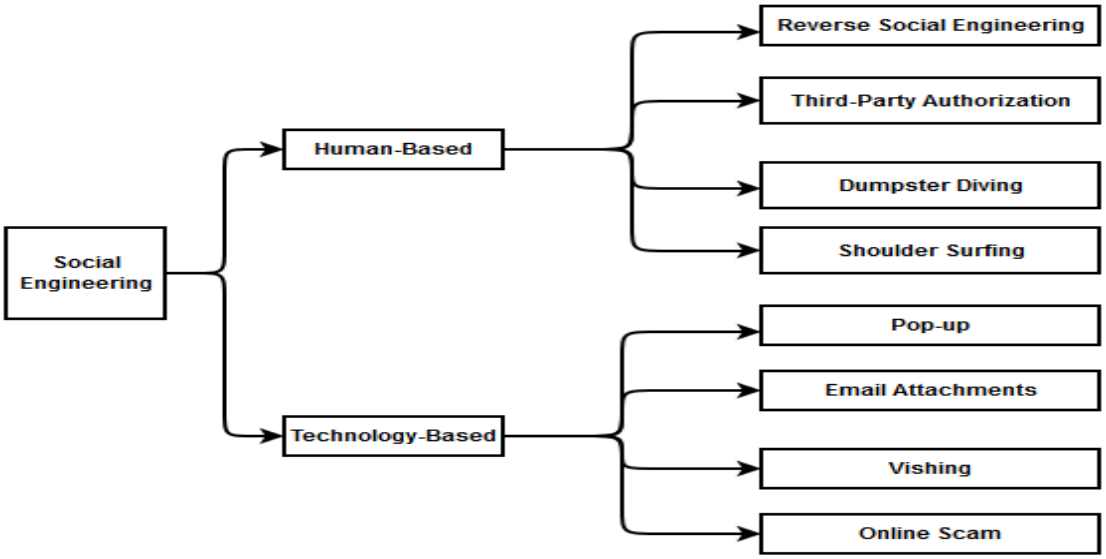

Figura 1.4. *Classificação dos Ataques de Engenharia Social,* (Janczewski, L. J.; Lingyan, F., 2010)

A classificação é semelhante à de Peltier (2006). Janczewski & Lingyan (2010), fazem referência às técnicas de *engenharia social inversa* e o *vishing*.

Na análise da figura 1.5 é possível observar-se que os autores na classificação começam por dividir os ataques em *Technical Hacking* e *Social Engineering*. Na classificação dos ataques de engenharia social, estes são agrupados em ataques de base-humana e de base-técnica.

Na referência às técnicas de base humana, em relação às abordadas anteriomente, não adicionaram nenhuma técnica nova. Na classificação dos ataques em base-técnica fazem referência ao *Signal Hijacking, Network Monitoring, Denial of Service (DoS) Digital Dumpster Diving, Theft Mobile Devices.* As técnicas referenciadas, excepto *Digital Dumpster Diving*, não são de fácil aplicação sendo necessário um conhecimento mais técnico.

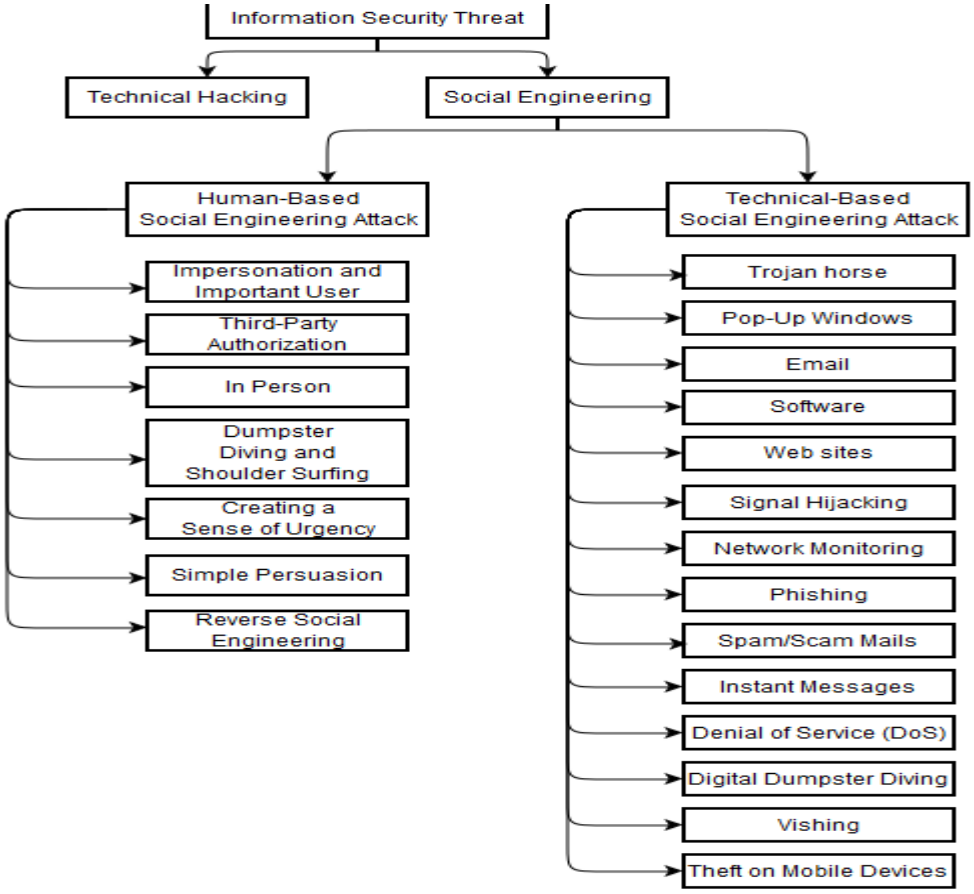

Figura 1.5. Classificação dos Ataques de Engenharia Social, (Foozy, Ahmad, Abdollah, Yusof, & Zaki, 2011)

O *Digital Dumpster Diving* comparativamente em relação à técnica *Dumpster Diving*, apresenta como diferença um é o lixo digital e o outro é o lixo "real". Pode ser definido como lixo digital todos os documentos ou ficheiros que são eliminados no computador e como lixo "real" todo o tipo de lixo físico, tais como recibos, facturas, extractos bancários, rascunhos, recibos, etc.

Na observação das classificações dos ataques de engenharia social em base-humana e base-técnica, propostas pelos diversos autores, observando-se alguns exemplos verifica-se que algumas das técnicas classificadas como de base-humana também podem ser classificadas como de base-tecnológica:

- A técnica *Shoulder Surfing*, de acordo com (Peltier, 2006)"*The shoulder surfer will look over someone's shoulder to gain passwords or pin numbers"*. Com a evolução das tecnologias a aplicação desta técnica passou a ser possível através da utilização de dispositivos electrónicos. Através da utilização de uma pequena câmara de filmar e de um equipamento de clonagem de cartões instalado na caixa multibanco, o engenheiro social consegue obter o código pessoal da vítima e a cópia do cartão de multibanco.

- (Peltier, 2006)descreve "*Dumpster divers (now called trash trawlers or garbologists) are willing to get dirty to get the information they need*". Na sua definição não teve em conta o lixo digital. Com base na categorização proposta por Peltier, o *Digital Dumpster Diving* é considerado como um ataque de base-técnica. O "lixo" digital muitas vezes contém informação confidencial.

A categorização dos ataques de engenharia social em base humana e base-técnica não é válida, como é possível observar através dos exemplos referenciados. Este tipo de classificação não permite acompanhar a evolução da tecnologia e das técnicas.

No âmbito da psicologia, sendo este um factor importante na engenharia social, constatou-se que os livros de Cialdini (2001) "*Influence: The Psychology of Persuasion"* e de Charles Lively (2004) "*Psychological Based Social Engineering*", abordados no capítulo 1.2, são as únicas referências na abordagem às condições humanas que são exploradas pelos engenheiros sociais. Cialdini descreve as seis condições utilizadas no desenvolvimento de um ataque e Charles Lively, baseando nas condições descritas por Cialdini (2001) anuncia os quatro vectores que são explorados. Estas obras são muito referenciadas em diversos estudos

.

1.7. OBJECTIVO DA DISSERTAÇÃO

1.7.1 Objectivo geral

Os objectivos a que nos propomos para a prossecução deste estudo, são:

1. caracterizar o conhecimento e a atitude dos utilizadores e dos responsáveis pelos SI nas empresas, relativamente à engenharia social e,
2. definir uma nova classificação dos ataques com base no tipo de abordagem.

Com vista a cumprir o primeiro objectivo, propomos responder às questões abaixo indicadas.

1.1. Em relação aos responsáveis pela segurança nas empresas, pretendemos identificar:

i. Com que entidades ou instituições utilizam a internet e o telefone para a realização de operações.
ii. Quais os serviços usados através do telefone e da internet.
iii. A formação dos responsáveis pela segurança.
iv. As medidas de segurança adoptadas.
v. O nível de conhecimento sobre a engenharia social
vi. O número de vítimas de ataque
vii. As técnicas de ataque mais utilizadas.
viii. Os principais alvos de ataque de engenharia social.
ix. A principal motivação dos ataques
x. A que entidades são participadas os ataques.
xi. Qual a abordagem de segurança adoptada depois do ataque.
xii. O nível de preocupação com a formação dos colaboradores
xiii. Qual o sentimento em relação aos riscos de segurança no futuro.
xiv. No futuro quais as plataformas que serão usadas nos ataques.

1.2. Em relação aos utilizadores pretendemos identificar:

i. Com que entidades ou instituições utilizam a internet e o telefone para a realização de operações
ii. Quais os serviços usados através do telefone e da internet.
iii. O nível de preocupação com segurança na utilização do telefone ou da internet na realização de operações.
iv. As medidas de segurança adoptadas
v. Qual a relação entre as medidas de segurança adoptadas e a idade.
vi. A proveniência do software antivírus.

vii. O nível de conhecimento sobre a engenharia social.
viii. Qual a relação entre o nível de conhecimento das técnicas de engenharia social e a idade.
ix. O número de vítimas de ataque
x. As técnicas de ataque mais utilizadas.
xi. A principal motivação dos ataques.
xii. As plataformas mais utilizadas na realização dos ataques.
xiii. A que entidades são participadas os ataques.
xiv. Qual o sentimento em relação aos riscos de segurança no futuro.
xv. No futuro quais as plataformas que serão usadas nos ataques
xvi. Qual a relação entre a disponibilização do correio electrónico com a idade e o género.

Com base na informação obtida, no ponto um, sobre os diferentes serviços e plataformas usadas no dia-a-dia, no nível de conhecimento e na atitude de segurança dos utilizadores e dos responsáveis TI nas empresas, existiu a necessidade de se propor uma nova forma de abordar a problemática da engenharia social.

Através da observação dos resultados obtidos, verificou-se que:

- o nível de conhecimento sobre as diferentes técnicas de ataque é reduzido,
- é baixo a diversidade das medidas de segurança que são aplicadas.
- na realização das suas actividades são diversos os serviços que são usados, aumentando desta forma o risco de serem vítimas de ataque

Com a multiplicidade dos serviços disponibilizados, muito resultado da evolução das tecnologias, os utilizadores estão vulneráveis a diferentes tipos de ataques. Os diferentes estudos, abordados no estado arte, limitam-se a distinguir os ataques em base humana e base-técnica não realçando os perigos existentes na utilização das diferentes plataformas de comunicação.

A nova proposta de classificação dos ataques de engenharia social baseada no tipo de abordagem, isto é, na forma de contacto entre a vítima e o atacante, pretende chamar a atenção dos utilizadores e dos responsáveis TI sobre os perigos na utilização das diferentes plataformas de comunicação, uma vez que, com o aumento da diversidade dos meios tecnológicos, os alvos de ataque de engenharia social multiplicam-se.

CAPÍTULO II – METODOLOGIA

O problema enunciado no Capítulo I remeteu-nos para a concepção de um trabalho de investigação que permitisse procurar respostas para as questões relacionadas com os perigos da engenharia social na segurança de informação. Neste capítulo será abordado a metodologia adoptada.

2.1. CARACTERIZAÇÃO DO ESTUDO

No desenvolvimento desta investigação foram utilizados dois questionários. Um dirigido aos utilizadores e o outro aos responsáveis pelos sistemas de informação (adiante "responsáveis de TIs") nas empresas (anexos I e II, respectivamente). Em ambos os inquéritos as questões são, na sua maioria, idênticas.

Tabela 2.1. Formulação do questionário aos responsáveis de TIs.

Tópico	Objectivo	Assuntos	Questões Formuladas
Os serviços utilizados	Identificar que organizações utilizam a internet e o telefone para a realização de operações Identificar quais os serviços que recorrem à Internet ou ao telefone para a realização de operações Identificar as vulnerabilidades	Quais os serviços que recorrem à Internet ou ao telefone para a realização de operações. Quais as organizações que utilizam a internet e o telefone para a realização de operações.	Identifique os serviços a que recorre à Internet ou ao telefone para a realização de operações?
Formação dos responsáveis de TIs	Identificar qual a área de formação dos responsáveis de TIs	Identificar entres os responsáveis de Tis qual a percentagem dos que são formados em cursos de tecnologias de informação. A identificação da área de formação dos responsáveis de TIs poderá justificar o nível de conhecimento demonstrado.	Identifique a sua área de formação?

Tópico	Objectivo	Assuntos	Questões Formuladas
Medidas de Segurança	Identificar as medidas de segurança aplicadas.	Os cuidados adoptados	Identifique quais as medidas de segurança que são aplicadas?
Ataques de engenharia social	Identificar o nível de conhecimento sobre os ataques de engenharia social. Determinar o número de vítimas de ataque de engenharia social. Identificar as técnicas de ataque mais utilizadas. Identificar qual principal motivação dos ataques.	O nível de conhecimento sobre as técnicas de ataque. O número de vítimas de ataque de engenharia social. As técnicas de ataque mais utilizadas Objectivo dos ataques	Já ouviram falar em ataques de engenharia social? Assinale os ataques de que já ouviram falar? Foram vitimas de algum tipo de ataque, ou ataques, de engenharia social? Identifique o tipo, ou tipos, de ataque de que foram alvo? Identifique o objectivo, ou objectivos, do ataque, ou ataques, de que foram alvo?
Alvos de Ataque	Identificar os principais alvos de ataque de engenharia social.	O nível de conhecimento sobre os possíveis alvos de ataque.	Identifique os possíveis alvos de ataque de engenharia social?
Atitudes adoptadas	Identificar a que entidades/autoridades são participados os ataques. Identificar qual a abordagem de segurança adoptada depois do ataque	Participação dos Ataques às autoridades. Abordagem de Segurança	Indique a que entidades participaram o ataque? Indique qual a abordagem de segurança adoptada depois do ataque?
Formação	Identificar o nível de preocupação com a formação dos colaboradores.	Formação dos colaboradores	Promovem acções de formação para os colaboradores?

Tópico	Objectivo	Assuntos	Questões Formuladas
Evolução dos Ataques	Identificar qual o sentimento em relação aos riscos de segurança no futuro. Identificar no futuro quais serão as plataformas usadas nos ataques.	Riscos de segurança no futuro	Qual o sentimento em relação aos riscos de segurança no futuro? Identifique no futuro quais serão as plataformas utilizadas nos ataques de engenharia social?

No inquérito aos utilizadores foi introduzido um campo para o fornecimento do endereço electrónico, não sendo este de preenchimento obrigatório. A principal razão da introdução desta questão no inquérito foi a de identificar, com base na idade e no género dos inquiridos, o grupo mais vulnerável a um ataque de engenharia social.

Tabela 2.2. Formulação do questionário dos utilizadores

Tópico	Objectivo	Assuntos	Questões Formuladas
Os serviços usados	Identificar com que organizações utilizam a internet e o telefone para a realização de operações Identificar quais os serviços a que recorrem através do telefone e da internet Identificar as vulnerabilidades	Quais os serviços que utilizam através do telefone e da internet. Quais as organizações com que realizam operações através da internet e do telefone.	Identifique os serviços a que recorre à Internet ou ao telefone para a realização de operações?
As preocupações com segurança	O nível de preocupação com a segurança na utilização do telefone ou da internet na realização de operações.	Qual a preocupação com a segurança na utilização dos meios de comunicação.	Quando realiza operações através do telefone ou internet preocupa-se com a segurança?

Tópico	Objectivo	Assuntos	Questões Formuladas
Medidas de Segurança	Identificar quais as medidas de segurança adoptadas	Os cuidados adoptados pelos utilizadores.	Identifique as principais medidas de segurança aplicadas.
	Identificar se existe alguma relação entre as medidas de segurança adoptadas e a idade dos utilizadores.		Idade?
	Identificar qual a proveniência do software utilizado.	A origem do software utilizado.	Indique a proveniência do software antivírus
Ataques de Engenharia Social	Identificar o nível de conhecimento sobre as técnicas de ataque de engenharia social.	O nível de conhecimento sobre as técnicas de ataque.	Já ouviu falar em ataques de Engenharia Social? Assinale as técnicas de que já ouviu falar?
	Identificar se existe alguma relação entre o nível de conhecimento das técnicas de engenharia social e a idade do utilizador	Caracterizar o nível de conhecimento dos utilizadores com base na idade	Idade?
	Identificar o número de vítimas de ataque	O número de vítimas de ataque de engenharia social.	Foi vítima de algum tipo de ataque de engenharia social?
		O número de ataques bem sucedidos	O ataque de que foi alvo foi bem-sucedido?
	Identificar as técnicas de ataque mais utilizadas	As técnicas de ataque mais utilizadas.	Identifique o tipo de ataque de que foi alvo.
	Identificar qual a principal motivação dos ataques	Objectivo dos ataques.	Identifique o principal objectivo do ataque de que foi alvo

Tópico	Objectivo	Assuntos	Questões Formuladas
Plataformas de Ataque	Identificar quais as plataformas mais utilizadas na realização dos ataques	As plataformas de ataque.	Indique qual a plataforma usada na realização do ataque
Atitudes adoptadas	Identificar a que entidades/autoridades são participados os ataques.	Participação dos ataques.	Indique a que autoridade participou o ataque
Evolução dos Ataques	Identificar quais as plataformas que serão usadas nos ataques, no futuro.	Riscos de segurança no futuro	Identifique quais serão no futuro as plataformas de ataque mais utilizadas.
	Identificar qual o sentimento em relação aos riscos de segurança no futuro.		Qual o sentimento em relação aos riscos de segurança no futuro?
Simulação de um ataque de engenharia social	Identificar qual a relação entre a disponibilização do correio electrónico com a idade.	Os possíveis alvos de ataque.	Idade? Email?
	Identificar qual a relação entre a disponibilização do correio electrónico e o género.		Género? Email?

2.2. SELECÇÃO DA AMOSTRA

Numa investigação "é impossível obter informação de todos os indivíduos ou elementos que formam parte do grupo que se deseja estudar; seja porque o número de elementos é demasiadamente grande, os custos são muito elevados ou ainda porque o tempo pode actuar como agente de distorção" (Richardson, 1999).

Na nossa pesquisa foram desenvolvidos dois inquéritos, um aos responsáveis de TIs e o outro aos utilizadores. Para o preenchimento dos inquéritos destinados aos responsáveis TI foram enviadas por correio electrónico cartas formais às instituições a solicitar o preenchimento do inquérito. Apenas foram recebidas 41 respostas ao pedido. São diversas as razões que poderão ter contribuído para uma reduzida amostra, podendo a principal estar relacionada com as politicas de segurança interna. Tal foi parcialmente atenuado pela intervenção, com recurso a relações de conhecimento e confiança pessoal e institucional, entre os orientadores deste trabalho e os responsáveis de TIs mencionados.

As amostras, dos inquéritos aos responsáveis TI, foram agrupadas de acordo com o sector de actividade. Entre os inquéritos obtidos, 83% pertencem ao sector terciário (Banca, Seguros, Telecomunicações, Organismos públicos e outros serviços). Por motivo da amostra ser reduzida, em relação aos restantes sectores de actividade, a investigação limitou-se ao estudo das actividades relacionadas, apenas, com o sector terciário.

O inquérito foi aplicado entre os dias 1 de Janeiro 2012 e 31 de Julho 2012. O universo dos utilizadores, alvo de estudo, que responderam ao inquérito é constituído por indivíduos com idade a partir dos 22 anos, residentes em Portugal e que frequentam as redes sociais. A amostra é constituída por 393 entrevistas, estratificadas por faixa etária, com a média de idades de 38 anos, dos quais 68% são do sexo feminino.

Tabela 2.3. Caracterização dos elementos da amostra com base no género e na faixa etária dos utilizadores

	Sexo	
Distribuição por faixa etária	Masculino	Feminino
22 a 34 anos	49	109
35 a 49 anos	65	120
mais 50 anos	13	37
Totais	**127**	**266**

2.3. INSTRUMENTOS UTILIZADOS

Na recolha de informação são classicamente assumidas dois tipos de técnicas: documentais e não documentais. Quando utilizando técnicas documentais, a recolha é feita a partir de suportes bibliográficos. Com a utilização de técnicas não documentais, o investigador pode realizar uma observação directa ou indirecta. A observação indirecta é efectuada pela aplicação de questionários.

O questionário é "*um instrumento de observação não participante, baseado numa sequência de situações escritas, que são dirigidas a um conjunto de indivíduos, envolvendo as suas opiniões, representações, crenças e informações factuais, sobre eles próprios e o seu meio*" (Quivy R. C., 1992).

Segundo (Tuckman, 2000), o questionário é utilizado pelos investigadores para transformar em dados a informação recolhida mediante interrogação de pessoas (ou sujeitos) e não observando-as ou recolhendo amostras do seu comportamento.
Antes do desenvolvimento de um inquérito é necessário saber a quem o queremos dirigir e o que queremos questionar. Na preparação das perguntas deve-se ter em conta a linguagem aplicada, o tipo de perguntas e a ordem pela qual ocorrem (Ghiglione & Matalon, 1992).

Considerando tal, o desenvolvimento do questionário foram utilizadas questões de resposta fechada onde o inquirido limita-se a selecionar a opção, entre as sugeridas, tendencial e desejavelmente, a que mais se adequa à sua opinião ou ao seu nível de conhecimento.

As questões de resposta vantagem apresentam um conjunto de características adequadas ao objeto sob estudo, ao universo considerado, aos meios de processamento das respostas existentes e à janela temporal disponível:

- mais adequadas ao tratamento estatístico das respostas;
- mais objectivas;
- de entendimento e resposta fácil para o inquirido;
- permitem garantir um certo anonimato.

Complementarmente, possibilitam a utilização de questões de resposta única ou questões de resposta múltipla (Ghiglione & Matalon, 1992).

No desenvolvimento do inquérito teve-se em atenção um conjunto de considerações desejáveis na elaboração de questionários dos utilizados. Nomeadamente, as seguintes:

- começar por uma pequena introdução sobre a entidade responsável pelo estudo e qual o seu objectivo;
- primeiras questões simples de forma a evitar o desinteresse do inquirido;
- introdução de perguntas mais objetivas no decorrer do questionário;
- questões tendencialmente curtas.

A utilização de questionários num processo de investigação pode trazer vantagens e limitações. Entre as vantagens destacam-se:

- facilidade de operacionalização, ao permitir a sua aplicação a uma amostra de grande dimensão num curto espaço de tempo;
- a reduzida, ou nula, exposição dos pesquisados;
- maior capacidade de sistematização dos resultados;
- melhor facilidade de análise e o reduzido custo que acarreta a sua aplicação.

Como instrumento de investigação apresenta também algumas limitações entre as quais as seguintes (Gil A. C., 2008) :

- exclui pessoas que não sabem ler ou escrever;
- a dificuldade existente na concepção das perguntas;
- a possível superficialidade das respostas;
- impossibilidade de ajudar o inquirido em questões mal compreendidas; e
- apenas ser passível de ser aplicado em populações homogéneas.

A Internet surge como um potenciador de uma difusão rápida do conhecimento, sendo tal também verdade para a condução de estudos como o conduzido. Para o investigador (Markham, 2004)" *the Internet provides new tools for conducting research* ".

A utilização da internet para a realização de inquéritos apresenta como vantagens: (Cohen, Manion, & Morrison, 2007):

- diminuição dos custos;
- diminuição do tempo de distribuição e recepção do questionário;
- diminuição do tempo de processamento;
- promoção de uma maior participação voluntária, o que resulta numa maior autenticidade nas respostas;
- uma maior diversificação dos inquiridos ;
- uma maior distribuição geográfica,
- respostas possível a partir de qualquer hora ou local.

Mesmo considerando a existência de algumas desvantagens da sua utilização (taxas de resposta muito baixas, dependência dos recursos tecnológicos, impessoalidade e menor selecção e qualidade da amostra (Gonçalves, 2008)), a realização da pesquisa subjacente a este trabalho com utilização da internet foi importante uma vez que permitiu chegar a um maior número de inquiridos e facilitou o processo de distribuição dos inquéritos e a recolha dos dados.

2.4. PROCEDIMENTO

Um trabalho de investigação é constituído por três etapas: fase exploratória; trabalho de campo e tratamento dos dados. Na fase exploratória são analisados os aspectos referentes ao objecto em estudo, aos objectivos a atingir, à metodologia a adoptar e às questões importantes para o desenvolvimento do trabalho de pesquisa. O trabalho de campo consiste no desenvolvimento de

técnicas de recolha de dados, pesquisas bibliográficas, inquéritos ou entrevistas. Por fim, faz-se o tratamento do material recolhido no trabalho de campo procedendo-se à sua organização e análise. (Minayo, 1994)

Na construção das questões foram tidas em conta as várias etapas preconizadas pelos diversos autores. Foi tido em conta a linguagem e a apresentação gráfica. Foram definidos os objectivos do questionário e a selecção dos meios disponíveis para a sua concretização. As questões inseridas foram resultado da observação e leitura de diversa bibliografia. Esta fase serviu para aprofundar o objectivo da investigação, pois é dela que todo o trabalho depende.

Os questionários foram sujeitos a apreciação por parte do orientador, de um modo geral positiva, tendo as sugestões produzido alguns ajustes considerados consensuais. Em ambos os questionários foram reformuladas algumas questões relativamente à linguagem utilizada.

Com o obectivo de se garantir que as respostas ao inquérito se limitam geograficamente a Portugal e em que não existe uma duplicação de respostas foi aplicada o método de filtragem por endereços IP. É sabido que tal filtragem não garante tal com total certeza, mas considerou-se que o grau de precisão era mais que suficiente para os objetivos do trabalho.

Para a solicitação do preenchimento do inquérito foi utilizado a rede social Facebook, que hoje interliga milhões de utilizadores. A utilização deste meio contribuiu para que o resultado da população da amostra uma vez que os indivíduos que responderam ao inquérito pertencem ao círculo da relação profissional, académico e pessoal.

Para a concretização de alguns dos objectivos os inquiridos foram agrupados de acordo com género e a faixa etária. Em algumas questões existiu a necessidade de identificar qual a relação entre o nível de conhecimento e a atitude do inquirido com a idade e o género. O objetivo subjacente a esta relação foi a definição de um perfil dos indivíduos.

Na selecção dos elementos da amostra com o objectivo de se identificar o conhecimento e a atitude dos utilizadores em relação à engenharia social foi aplicada uma filtragem com base na resposta à questão - *Já ouviu falar em ataques de Engenharia Social?*. Os inquiridos que responderam – *Não* – foram excluídos na análise das questões.

Os dados obtidos no inquérito permitirão desenvolver uma caracterização da população que frequentam as redes sociais, em relação à problemática da engenharia social.

2.5. ANÁLISE DOS DADOS

A análise dos dados é mais uma etapa no processo de investigação. "*A análise tem como objectivo organizar e sumariar os dados de tal forma que possibilitem o fornecimento de respostas ao problema proposto para investigação*" (Gil A. C., 1999).

Miranda (1999) define os dados como "*um conjunto de registos qualitativos ou quantitativos conhecido que organizado, agrupado, categorizado e padronizado adequadamente transforma-se em informação*" (Miranda, 1999).

Para o tratamento dos dados, utilizou-se como base de análise a estatística descritiva. Na análise estatística iremos determinar qual a margem de erro da amostra para um intervalo de confiança de 95%. Os resultados serão analisados com apoio na utilização de gráficos.

Seja:
n – o tamanho da amostra
$\bar{X}$ – média amostral
μ - média populacional
σ – desvio padrão
z - variável normal padronizada
IC – intervalo de confiança
(1 – α) – o nível de confiança

A determinação da margem de erro será feita através da utilização da fórmula:

$$IC_{(1-\alpha)}(\mu) = \left(\bar{X} - z_{1-\alpha/2} \frac{\sigma}{\sqrt{n}}, \bar{X} + z_{1-\alpha/2} \frac{\sigma}{\sqrt{n}} \right)$$

Figura 6. Cálculo do IC para μ com grau de confiança 1-α (Jordán, Gladys Castillo, 2008)

CAPÍTULO III – RESULTADOS E DISCUSSÃO

Neste capítulo são apresentados e analisados os resultados à investigação efectuada atendendo aos objectivos definidos no capítulo II. Optou-se por analisar separadamente os resultados de forma a permitir uma melhor organização dos dados.

Dividiu-se o capítulo em dois subcapítulos, sendo no primeiro analisados os dados relativos ao inquérito aos responsáveis TI e no segundo subcapítulo os referentes ao inquérito aos utilizadores.

A partir dos dados obtidos tentaremos caracterizar, sobre um conjunto de questões, os utilizadores e os responsáveis TI.
Os dados serão analisados com o objectivo de identificar principalmente 3 vectores:

- qual o nível de conhecimento dos responsáveis pelos sistemas de informação e dos utilizadores sobre a engenharia social;
- quais as plataformas e as técnicas de ataques mais utilizadas em Portugal: e
- quais as atitude de segurança adoptadas.

3.1. ANÁLISE DOS RESULTADOS DO QUESTIONÁRIO APLICADO AOS RESPONSÁVEIS TI.

Os inquéritos obtidos foram agrupados de acordo com o sector de actividade tendo 89% origem no sector terciário.

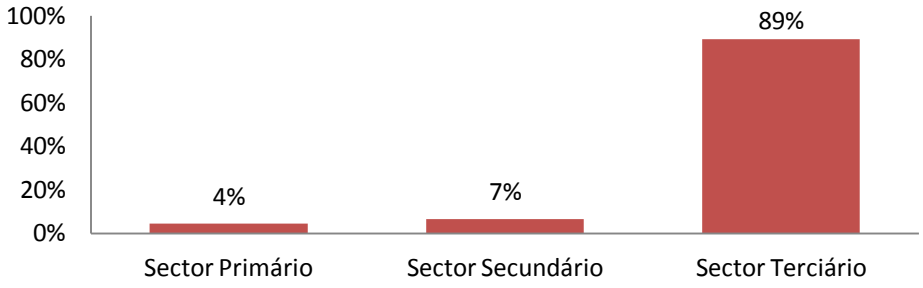

Gráfico 3.1. Descrição das empresas que responderam ao inquérito de acordo com sector de actividade

Devido à reduzida dimensão das amostras relativas aos outros sectores de actividade, a investigação focará, apenas, os inquéritos referentes ao sector terciário. Este sector abrange o

ramo financeiro, seguros, telecomunicações e serviços, claramente os mais expostos e com maior dependência da utilização de tecnologias de informação e comunicação.

A partir das entrevistas realizadas verificou-se que entre os inquiridos que responderam ao inquérito, apenas 39% são especialistas em Tecnologias de Informação. Este facto poderá ser importante na análise das respostas pois permitirá identificar as diferenças no conhecimento e nas atitudes de segurança existentes entre os formados em tecnologias de informação e os restantes. Foram entre as empresas de grandes dimensões que a maioria dos inquéritos foram respondidos por especialistas TI.

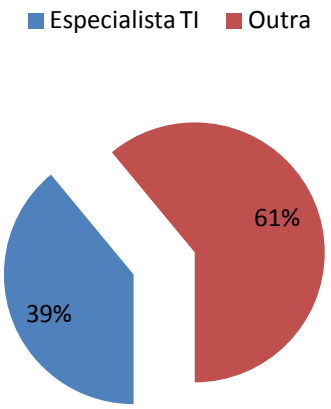

Gráfico 3.2. Identificação da formação

Os resultados da amostra são pouco significativos em relação aos ramos: financeiro, seguros, comunicações e administração pública.

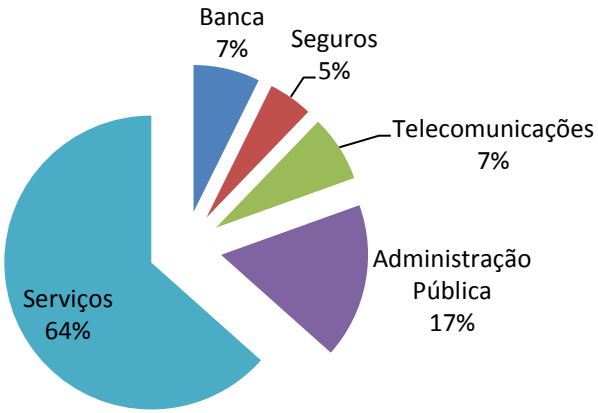

Gráfico 3.3. Descrição das actividades do sector terciário

A maioria dos inquéritos está relacionada com as actividades do ramo de serviços. As restantes actividades, no seu conjunto, correspondem a menos de 40% dos inquéritos recolhidos.

3.1.1. Identificação dos principais serviços utilizados

As empresas no desenvolvimento das suas actividades utilizam a Internet e o telefone como meios de comunicação. A partir da análise do gráfico 3.4 abaixo é possível observar os diversos serviços utilizados através destes meios.

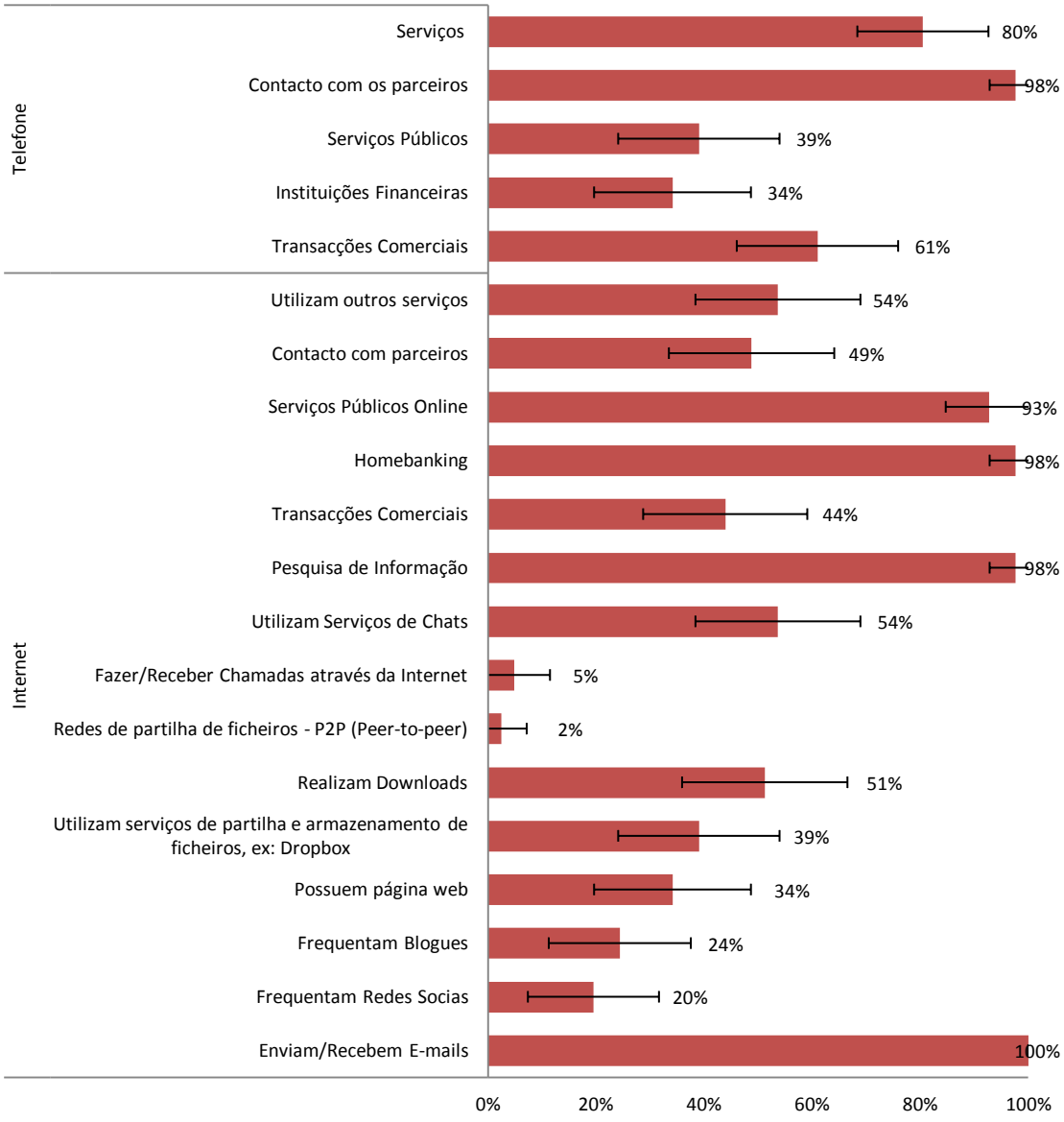

Gráfico 3.4.Resultado das respostas, quando questionados sobre quais os serviços que utilizam, com intervalo de confiança de 95%. As margens de erro estão indicadas para cada serviço apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 1)

De acordo com os dados disponibilizados pela PORDATA (2012), a taxa de utilização da internet pelas empresas, com 10 e mais pessoas ao serviço, era de 98%. Entre as diversas actividades desenvolvidas através da internet, o processamento de emails (envio e recepção) e a pesquisa de informação são as actividades mais utilizadas, sendo no contacto com os organismos públicos e com as instituições financeiras a internet o meio preferencial.

Com a crescente importância da utilização deste meio, os ataques têm sido orientados à exploração das suas vulnerabilidades. Na utilização dos diversos serviços - email, contactos *online* com as instituições financeiras e organismos públicos, serviços de conversação – (vulgo *chat*), downloads, entre outros - as empresas estão vulneráveis a diversos tipos de ataque - *malware*, *spying*, *phishing*, *interesting software*, *hoaxing*, *pop-ups*, etc. No capítulo seguinte este assunto será abordado.

Por exemplo, na utilização dos serviços de email, as instituições estão vulneráveis a ataques, nomeadamente, de *malware*. Uma infecção por vírus poderá ter como consequência a instalação de *backdoors* de forma a garantir a terceiros mal intencionados o acesso e o controlo da máquinas infectada, com potencial revelação de informação e ainda a realização de ataques a outros sistemas a partir das primeiras.

Num outro registo, é reconhecido por todos que as empresas, com o objectivo de reduzirem os custos com o armazenamento de informação, estão a recorrer aos serviços de armazenamento e partilha de ficheiros na nuvem – *cloud*. Pela observação do gráfico 3.4 é possível verificar que 39% das empresas recorrem a estes serviços.

Na sua utilização, as instituições entregam a gestão da sua informação a terceiros perdendo o controlo sobre os processos que estão em execução ou onde os dados estão armazenados. Antes de aderirem a estes serviços os clientes de forma a reduzirem os riscos, associados à sua utilização, devem certificar que o fornecedor garante a integridade, disponibilidade, confidencialidade, autenticidade e o não-repúdio da informação.

De acordo com o estudo desenvolvido pela ISACA, que abrangeu mais de 1500 companhias de mais de 50 países da Europa, Médio Oriente e África, uma em cada cinco empresas clientes de *cloud computing* desvalorizam os riscos da utilização da tecnologia. Perto de dois terços mostraram-se disponíveis a assumirem um determinado nível de risco, (12%) dos responsáveis de TI dizem-se dispostos a assumir os riscos para maximizar o retorno de negócio.

Na análise dos serviços que são utilizados através do telefone, verifica-se que este é o meio de preferencial no contacto com os parceiros (98%), estando a este canal associada a possibilidade de concretização de vários tipos de ataques - *impersonation/pretexting*, *smishing*, *vishing*, entre outros.

Ao incluir-se na análise a utilização dos *smarthphones*, deve-se adicionar os ataques associados à utilização da internet, uma vez que este tipo de equipamentos permite o acesso ao serviço.

3.1.2. As medidas de segurança aplicadas

A segurança deverá ser a uma forte preocupação das empresas no desenvolvimento das suas actividades, sendo nesse sentido necessário o desenvolvimento de políticas de segurança que permitam garantir a integridade, confidencialidade e a disponibilidade da informação.

Quando questionados sobre quais as medidas de segurança implementadas, mais de 60% indicaram como principais medidas, um conjunto reduzido comum:

- a instalação de soluções antivírus;
- a utilização de uma firewall;
- a actualização do software;
- a destruição dos documentos; e
- a não utilização de *pens-usb* externas.

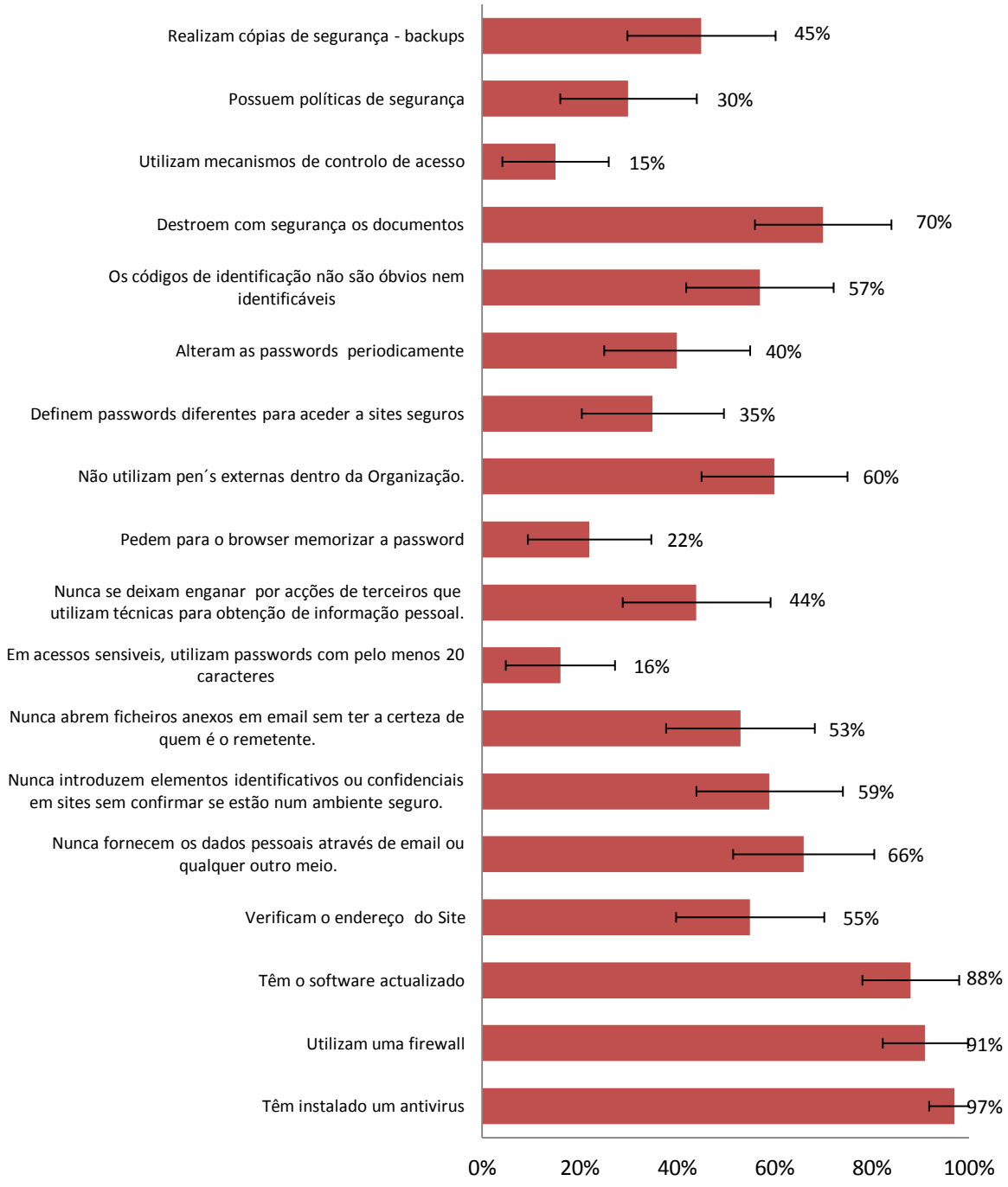

Gráfico 3.5. Resultado das respostas quando questionados sobre quais as medidas de segurança adoptadas, com intervalo de confiança de 95%. As margens de erro estão indicadas para cada serviço apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 2)

Em relação às medidas mencionadas no gráfico 5, chama-se a atenção para a preocupação com a destruição dos documentos e com a utilização das *pens-usb* externas dentro da organização.

- Destruição de documentos - A destruição dos documentos é um problema com que as empresas se deparam e a que não dão, tipicamente, a devida importância. Efetivamente, o maior perigo associado à não destruição da informação, de forma adequada (no sentido de "com segurança"), reside na perda da confidencialidade. O problema reside no perigo da informação cair nas mãos de alguém mal-intencionado, uma vez que poderá ser usada na realização de um ataque. O Dumpster Diving é uma técnica, de engenharia social, que consiste no recurso ao lixo como fonte de informação.

- Dispositivos móveis - As empresas, na utilização dos dispositivos móveis de armazenamento de dados – tipicamente associados aos dispositivos do tipo *pens-usb* - deverão ter em atenção os perigos associados à sua utilização. O primeiro está relacionado com a perda destes dispositivos e, consequentemente , a perda da própria informação da empresa. O segundo está relacionado com a utilização de *pens-usb* externas dentro da organização que poderão resultar em ataques de *baiting*, *malware*, spying, entre outros.

Através da observação do gráfico verifica-se que existe um conjunto de medidas que são aplicadas por menos de 50% das empresas, destacam-se as preocupações com as cópias de segurança, com as passwords e com o controlo de acessos.

- Backups - Os *backups* – ou cópias de segurança - são uma importante medida de segurança, que deverão ser implementados não só para recuperar a informação no caso de perda acidental seja por falha física ou por falha humana, mas também da consequência de uma possível infecção por vírus ou de uma invasão. Esta medida é aplicada por apenas 45% das empresas;

- Passwords - As empresas, no desenvolvimento das suas políticas de segurança, deverão definir regras na utilização de passwords. As regras deverão ter em atenção a dimensão, a composição, a validade e, de forma não menos importante, a exclusividade da password.

  A password é um elemento importante na identificação de um utilizador perante um sistema ou rede. Quando questionados sobre a dimensão, a validade e a exclusividade das passwords, 16% indicaram que utilizam passwords com pelo menos 20 caracteres, 40% alteram-nas periodicamente e 35% utilizam passwords diferentes para aceder a

sites seguros. Na referência à utilização de passwords com pelo menos 20 caracteres, a medida é de duvidosa aplicação;

- Em relação à implementação dos mecanismos de controlo de acessos, uma medida que poderá contribuir para impedir a execução de um conjunto de técnicas de engenharia social, abordadas no capítulo I, entre elas o tailgating, constata-se que somente 15% das empresas a implementam.

Da análise deste gráfico é ainda possível observar que apenas 30% das empresas possuem políticas de segurança, algo que é preocupante.

As políticas de segurança têm um papel determinante na segurança das organizações, uma vez que é através delas que são descritas um conjunto de regras e procedimentos que irão permitir reduzir as vulnerabilidades e as ameaças.

Por fim, é inquietante verificar-se que entre os responsáveis TI cerca de 40% afirmam "*nunca se deixam enganar por acções de terceiros que utilizam técnicas para obtenção de informação pessoal",* o que demonstra um total desconhecimento sobre as características dos ataques de engenharia social. A medida "*pedem ao browser para memorizar a password*" não poderá ser considerada uma medida de segurança no sentido em que existem na internet aplicações que permitem obter a informação armazenada.

3.1.3. O nível de conhecimento sobre a engenharia social.

Através da análise do gráfico 3.6 verifica-se que, entre o universo dos inquiridos, 88% afirmaram ter ouvido falar em ataques de engenharia social.

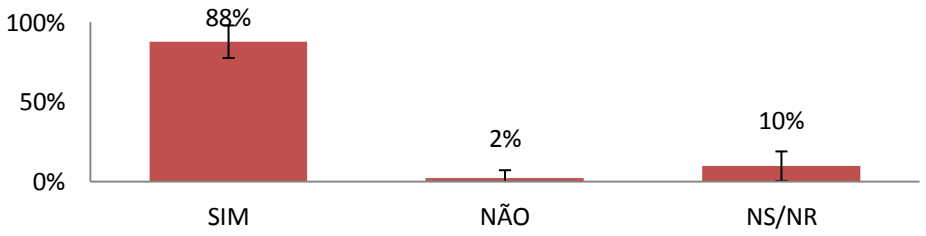

Gráfico 3.6. Resultado das respostas quando questionados: " Se já ouviram falar em ataques de engenharia social", com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 3)

Quando questionados sobre quais as técnicas de ataque que já ouviram falar (gráfico 3.7), é possível constatar que as técnicas malware, *spam-mail*, *phishing e o pop-up* são as mais conhecidas. A técnica *vishing*, uma variante do *phishig*, é conhecida por, apenas, 13% dos responsáveis TI.

É importante referir que entre as 17 técnicas de ataque de engenharia social abordadas, apenas 4 são conhecidas por mais de 50% dos responsáveis TI, constatando-se também que os ataques mais conhecidos são os que são mais referenciados nos meios de comunicação.

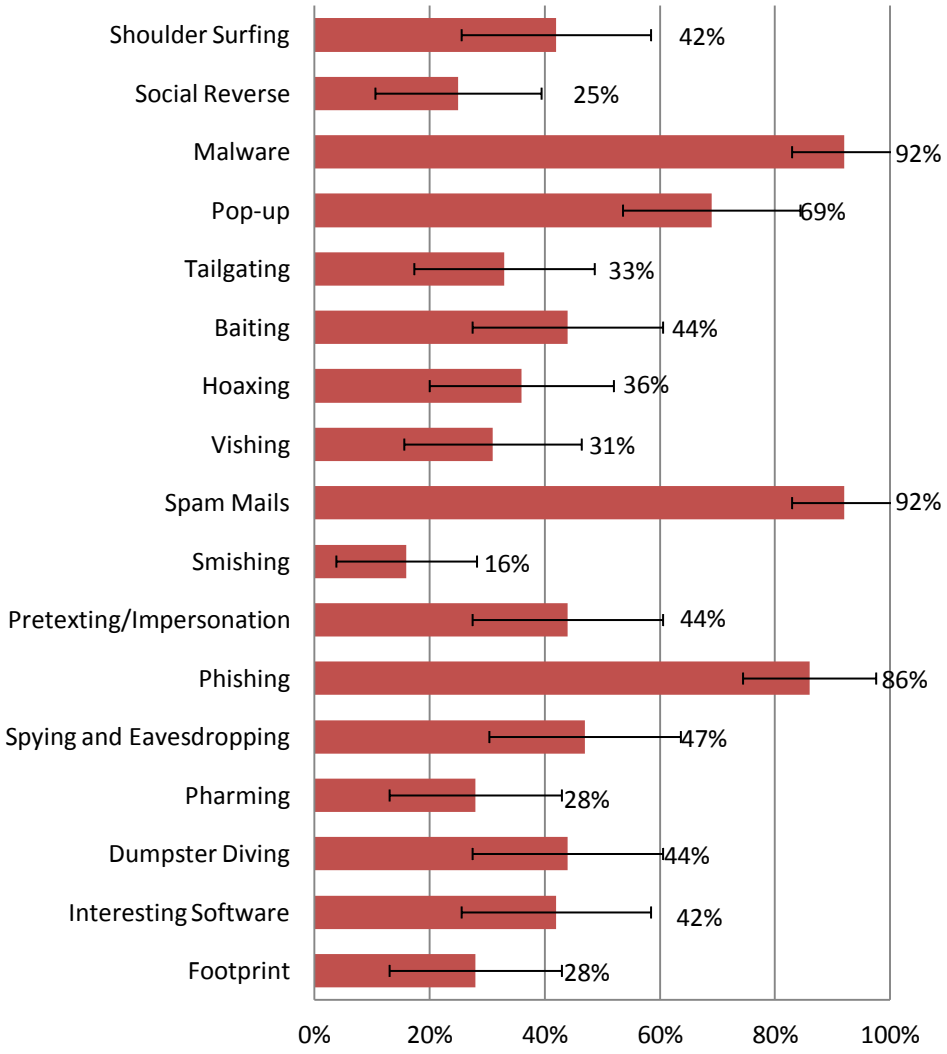

Gráfico 3.7. Resultado das respostas quando questionados: "*Assinale os ataques de que já ouviu falar?*", com intervalo de confiança de 95%. As margens de erro estão indicadas para cada técnica de ataque apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 4)

3.1.4. As técnicas de ataque mais utilizadas

Na análise do gráfico 3.8 é possível constatar que entre os responsáveis TI, que já ouviram falar em ataques de engenharia social, (83%) afirmaram terem sido alvo de ataque.

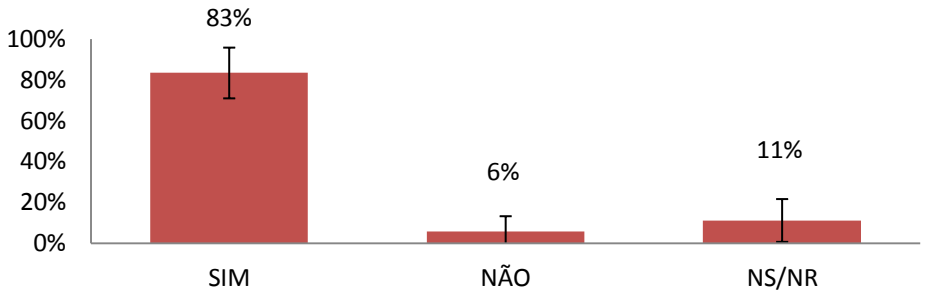

Gráfico 3.8. Resultados das respostas quando questionados: "Se já s*ofreram algum tipo de ataque de engenharia social?*", com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 5)

Na identificação das técnicas de ataque de que foram alvo, pela observação do gráfico 3.9, verifica-se que o *spam-mails*, *malware* e o *phishing* são as técnicas de ataque mais utilizadas. Na análise desta questão só foram tidas em conta as respostas dos que afirmaram terem sido alvo de ataque de engenharia social.

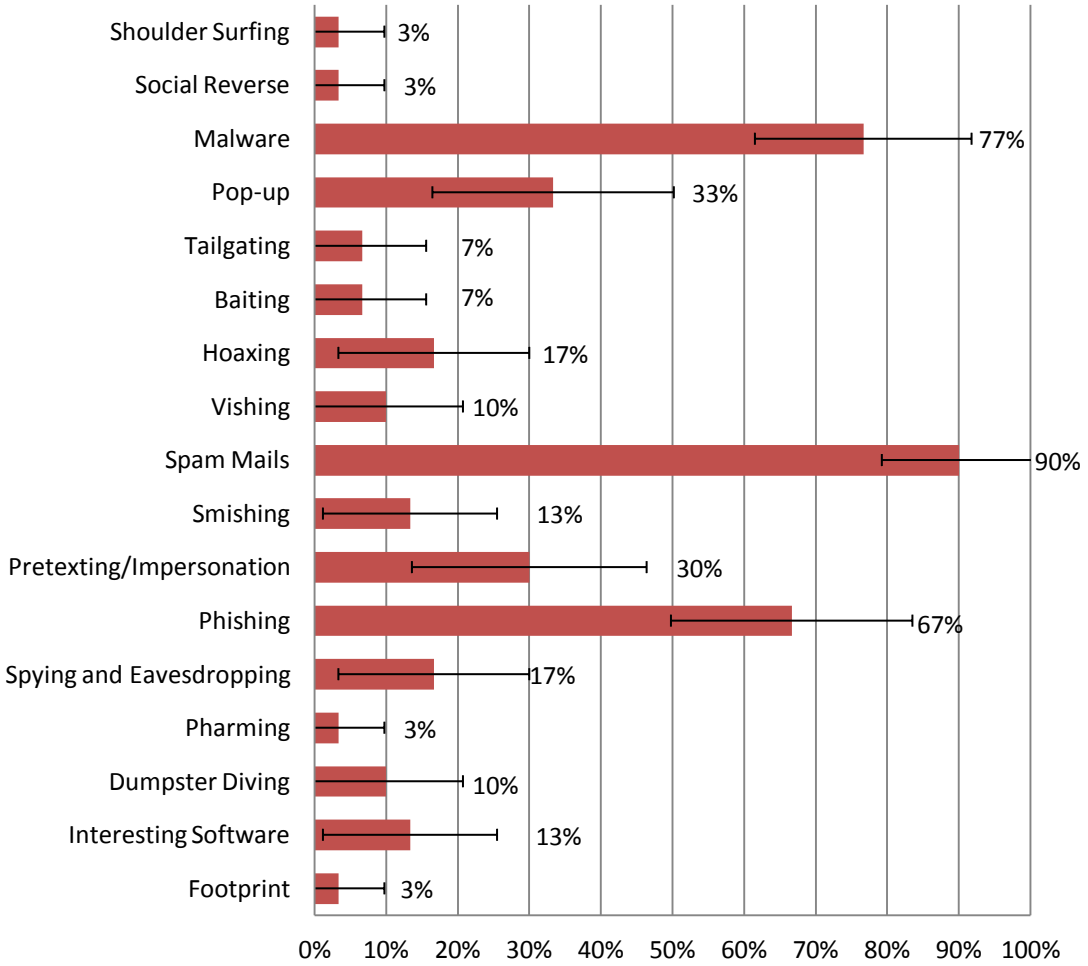

Gráfico 3.9. Resultado das respostas quando questionados para identificar o tipo de ataque de que foram alvo, com intervalo de confiança de 95%. As margens de erro estão indicadas para cada técnica de ataque apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 6)

3.1.5. Os principais alvos de ataques de engenharia social

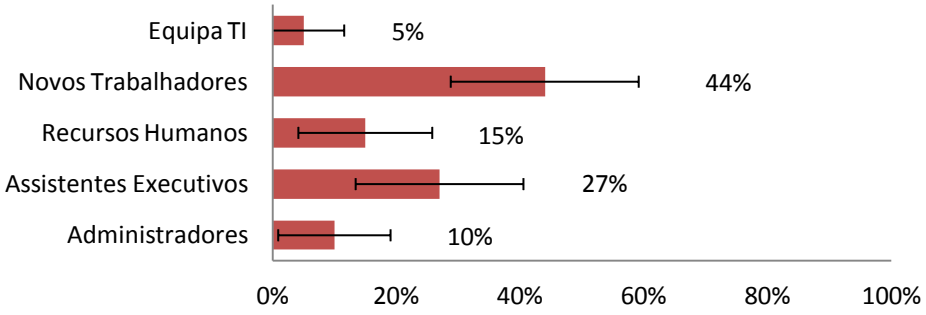

Gráfico 3.10. Resultado das respostas quando questionados para identificarem, entre os colaboradores, os principais alvos de ataques de engenharia social, com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 7)

Quando questionados para identificarem, entre os colaboradores, os possíveis alvos de ataque de engenharia social, (44%) indicaram os novos trabalhadores como os mais vulneráveis, por ainda não estarem familiarizados com as políticas de segurança, pela necessidade de se sentirem úteis e pela insegurança na forma de actuar. Os assistentes executivos são um outro grupo alvo de ataques por possuírem um maior acesso à informação.

3.1.6. A principal motivação dos ataques

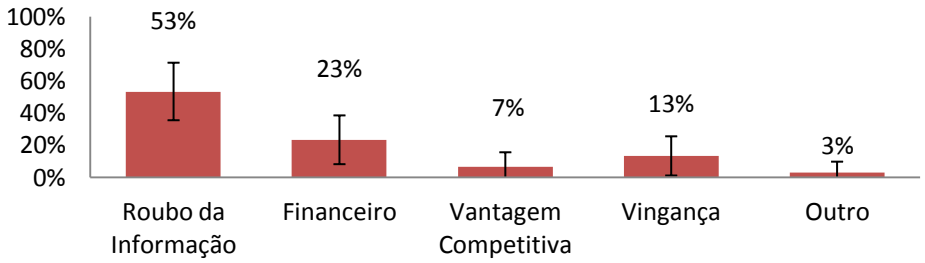

Gráfico 3.11. Resultado das respostas quando questionados para identificar o principal objectivo do ataque, com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 8)

Na identificação da principal motivação dos ataques, a maioria indicou o roubo de informação. O motivo dos ataques pode variar de local para local, verificando-se nas seguintes geografias as respectivas razões principais (Research Dimensional, 2011):

- Austrália e nos Estados Unidos - roubo financeiro;
- Alemanha - vingança;
- Canadá – concorrência.

3.1.7. Participação dos ataques

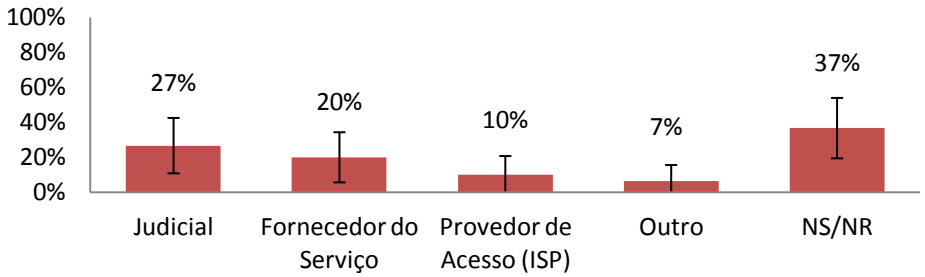

Gráfico 3.12. Resultado das respostas quando questionados se após sofrerem um ataque efectuaram alguma participação a alguma autoridade, com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 9)

Quando questionados (identificação) sobre a atitude dos responsáveis TI depois de um ataque, a maioria dos inquiridos não aceitaram responder à questão. Entre os que responderam, (27%) afirmaram ter participado o ataque a uma autoridade judicial.

3.1.8. A abordagem de segurança.

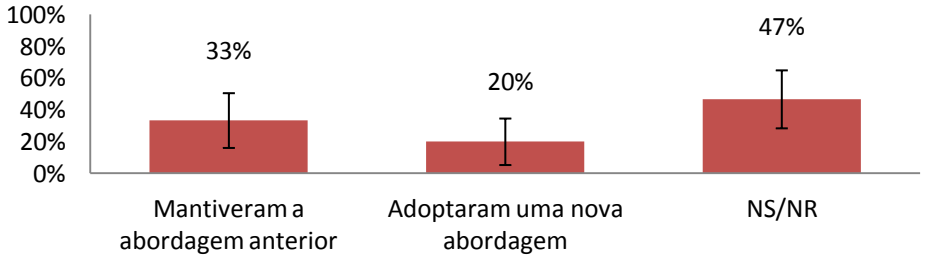

Gráfico 3.13. Resultado das repostas quando questionados sobre qual a abordagem aplicada depois do ataque, com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 10)

Com o objectivo de identificar sobre qual a abordagem de segurança adoptada depois de sofrerem um ataque de engenharia social, (33%) afirmaram ter mantido a mesma abordagem. A maioria dos inquiridos não aceitou responder à questão por trás desta atitude poderão estar diversos motivos, entre eles, motivos de segurança.

3.1.9. Formação dos colaboradores

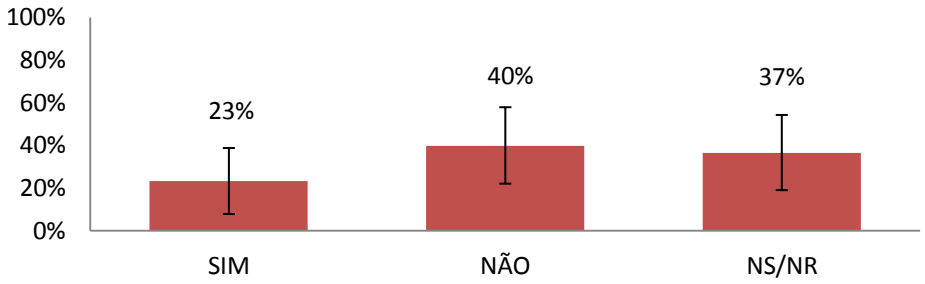

Gráfico 3.14. Resultado das respostas dadas quando questionados se promovem acções de formação dos colaboradores sobre os ataques de engenharia social, com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 11)

Entre as diversas medidas que deverão ser adoptadas com o objectivo de reduzir a probabilidade de sucesso de um ataque de engenharia social, a principal medida deverá passar pela formação dos colaboradores. Através da análise do gráfico verifica-se que a preocupação com a formação não é uma prioridade para as empresas. Entre os que responderam, apenas (23%) afirmaram ter desenvolvido acções de formação para os colaboradores.

3.1.10. O sentimento em relação aos riscos de segurança no futuro

Na identificação do sentimento em relação aos riscos de segurança no futuro, verifica-se que a maioria dos responsáveis TI pensa que os riscos tenderão a piorar.

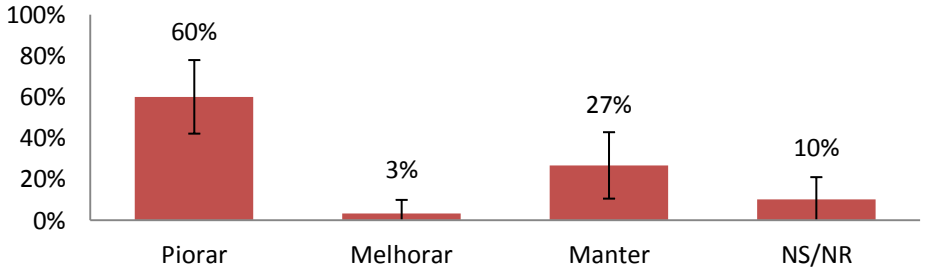

Gráfico 3.15. Resultado das respostas dadas quando questionados sobre qual o sentimento em relação aos riscos de segurança no futuro, com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 12)

Quando convidados para identificarem no futuro quais serão as plataformas de ataque mais utilizadas, segundo os responsáveis TI as redes sociais tenderão a ser a principal plataforma de ataques de engenharia social.

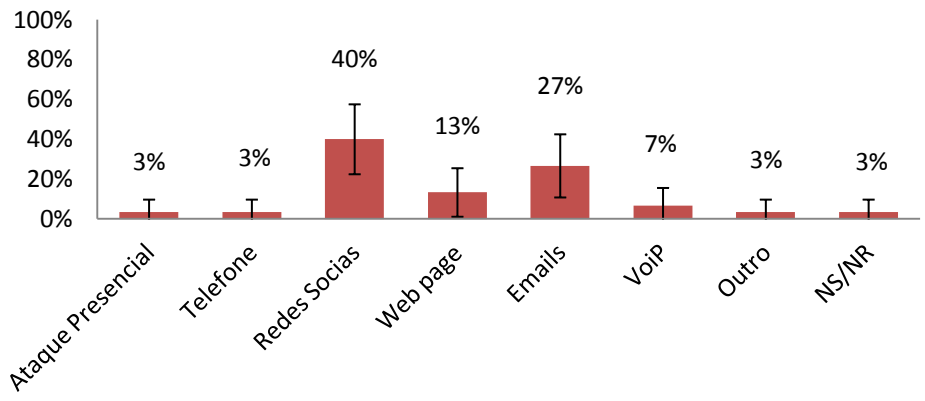

Gráfico 3.16. Resultado das respostas dadas quando questionados para identificarem no futuro quais serão as plataformas mais utilizadas nos ataques de engenharia social, com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 13)

De acordo com Kevin Haley, especialista do *Security Response* da Symantec, sobre as previsões de segurança para 2013, os riscos de ataque tenderão para: conflitos cibernéticos; aparecimento do Ransomware; surgimento de malwares para dispositivos móveis – madwares; golpes ligados às redes sociais e ataques às plataformas móveis e aos serviços de nuvem.

- Em relação aos ataques cibernéticos, Kevin afirma que os conflitos entre as nações, organizações e indivíduos tenderão a ser desenvolvidos no mundo virtual. A aplicação da técnica de espionagem, no mundo virtual, poderá ser bem-sucedida.

- Novos malwares surgirão, entre eles, o *Ramsomware* e o *Madware*. Os *Ramsomwares* são um tipo de ataque que consiste na utilização de um software mal-intencionado que bloqueia o computador e exige uma taxa de resgate para o desbloquear.

- Os dispositivos móveis cada vez mais são usados dentro e fora das redes corporativas, contendo dados e informações confidenciais aumentam os riscos da segurança de informação e despertam o interesse no desenvolvimento de ataques. O *Madware* é um tipo de malware desenvolvido para os dispositivos móveis, que tem como objectivo recolher informações. Este tipo de ameaça instala-se nos dispositivos através dos *downloads* de aplicações. Este tipo de ataque só nos últimos nove meses aumentou (210%).

3.2. ANÁLISE DOS RESULTADOS DO QUESTIONÁRIO APLICADO AOS UTILIZADORES.

3.2.1. Caracterização dos inquiridos

(Paisana & Lima, 2012) na identificação do nível de utilização da Internet, "*descreve que a taxa de utilização decresce à medida que a idade aumenta e a escolaridade diminui (90,6%) dos inquiridos entre os 15 e os 24 anos utilizam a Internet, contra (5,0%) dos que têm 65 ou mais anos; (97,5%) dos inquiridos com Instrução Primária incompleta não utilizam a Internet, enquanto que (96,9%) dos Universitários / Pós-graduados / Doutorados utilizam este meio de comunicação)* "

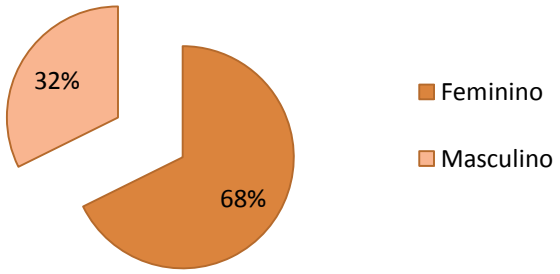

Gráfico 3.17.Caracterização da amostra em termos de género.

Na investigação foram obtidas 393 amostras. Dos indivíduos que responderam ao inquérito, (68%) são do sexo feminino. A média de idades da amostra ronda os 38 anos, representando a faixa entre os 22 e os 49 anos (87%) dos inquiridos.

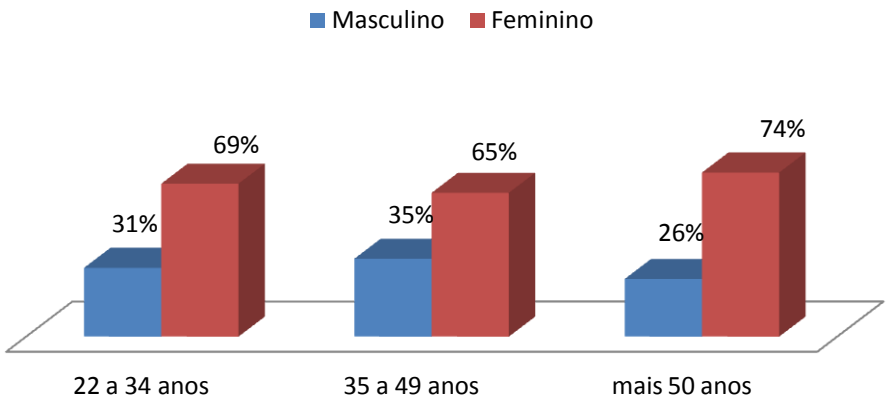

Gráfico 3.18. Caracterização da amostra com base no género e na faixa etária

"*Dos homens portugueses, (54,3%) eram em 2011 utilizadores de Internet, enquanto nas mulheres a parcela de internautas era de (44,2%). A utilização de Internet apresenta uma tendência a diminuir em sentido inverso da idade: é na faixa dos 15 aos 24 anos que se encontra a maior parcela de utilizadores de Internet (90,6%), ligeiramente inferior no escalão seguinte, dos 25 aos 34 anos (79,2%). À medida que a idade sobe a tendência acentua-se, sendo o grau de não utilização muito alto nos escalões etários dos 55 - 64 anos (71,0%) e 65 e + anos (93,9%)"* (Paisana & Lima, 2012) .

Relativamente à ocupação profissional, verifica-se "*maior concentração de utilizadores de Internet nos quadros superiores (100%), profissionais liberais (100%), profissões técnicas, científicas e artísticas (98%), estudantes (97,4%) e empregados de escritório (90,2%). Os grupos com menor incidência no que se refere à utilização de Internet são os reformados/pensionistas (9,2%) e domésticas (8,6%)"* (Paisana & Lima, 2012)

No desenvolvimento da investigação optou-se por analisar algumas questões, estratificando os inquiridos com base na faixa etária, com o objectivo de se identificar diferenças no conhecimento e na atitude dos inquiridos que possam estar relacionadas com a idade.

3.2.2. Caracterização dos inquiridos que indicaram o email, quanto ao género e à faixa etária.

Foi solicitado aos utilizadores, em sede de preenchimento do inquérito, que indicassem o seu endereço de email, sendo que para o prosseguimento do questionário a questão não fosse de preenchimento obrigatório. A utilização desta questão teve por objectivo identificar um perfil de (possíveis) alvos de um ataque bem-sucedido.

Através da utilização do email, abordado no capítulo I, são diversos os tipos de ataque de engenharia social que poderão ser desenvolvidos. Ilustrativamente, poder-se-ia enviar um agradecimento aos utilizadores que disponibilizaram o endereço de correio-electrónico - pela disponibilidade no preenchimento do inquérito – com um *link* para um site com os resultados do estudo que, automática e paralelamente, tentaria atacar os browsers dos utilizadores.

De acordo com Charles Livelly, abordado no capítulo I, um engenheiro social no desenvolvimento de um ataque, tende a explorar, entre outros vectores, a necessidade do ser humano em sentir-se útil.

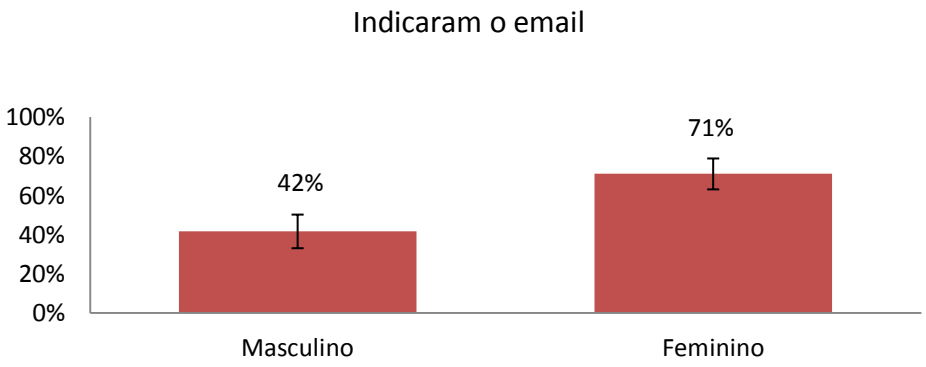

Gráfico 3.19. Caracterização dos inquiridos que indicaram o email com base no género, com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 14)

Através da observação do gráfico 3.19 é possível verificar que os utilizadores do sexo feminino são os mais vulneráveis a um ataque de engenharia social.

Ao analisar-se as possíveis vítimas de ataque, com base na faixa etária, é possível observar, através do gráfico 3.20, que os indivíduos com mais de 50 anos são os mais vulneráveis.

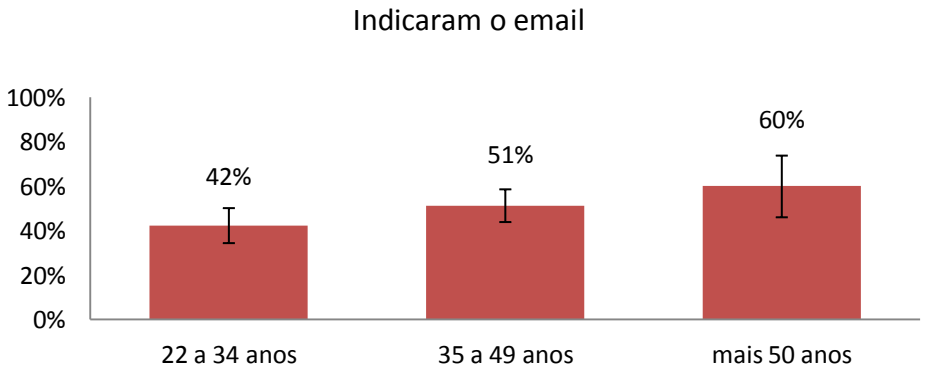

Gráfico 3.20. Caracterização dos inquiridos que indicaram o email com base na idade, com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 15)

3.2.3. Identificação dos principais serviços utilizados

Hoje, a informação é um factor importante no desenvolvimento da sociedade e da pessoa. Com a evolução das tecnologias surge um conjunto de novas plataformas de comunicação que permitem eliminar as distâncias e estabelecer novas formas de comunicar, de relacionar e de partilha de informação.

Com a evolução das plataformas de comunicação e com a utilização dos novos serviços disponibilizados, surgem também novos alvos de ataque. Na análise do gráfico 3.21 é possível identificar alguns dos serviços disponíveis na utilização do telefone e da internet como meios de comunicação.

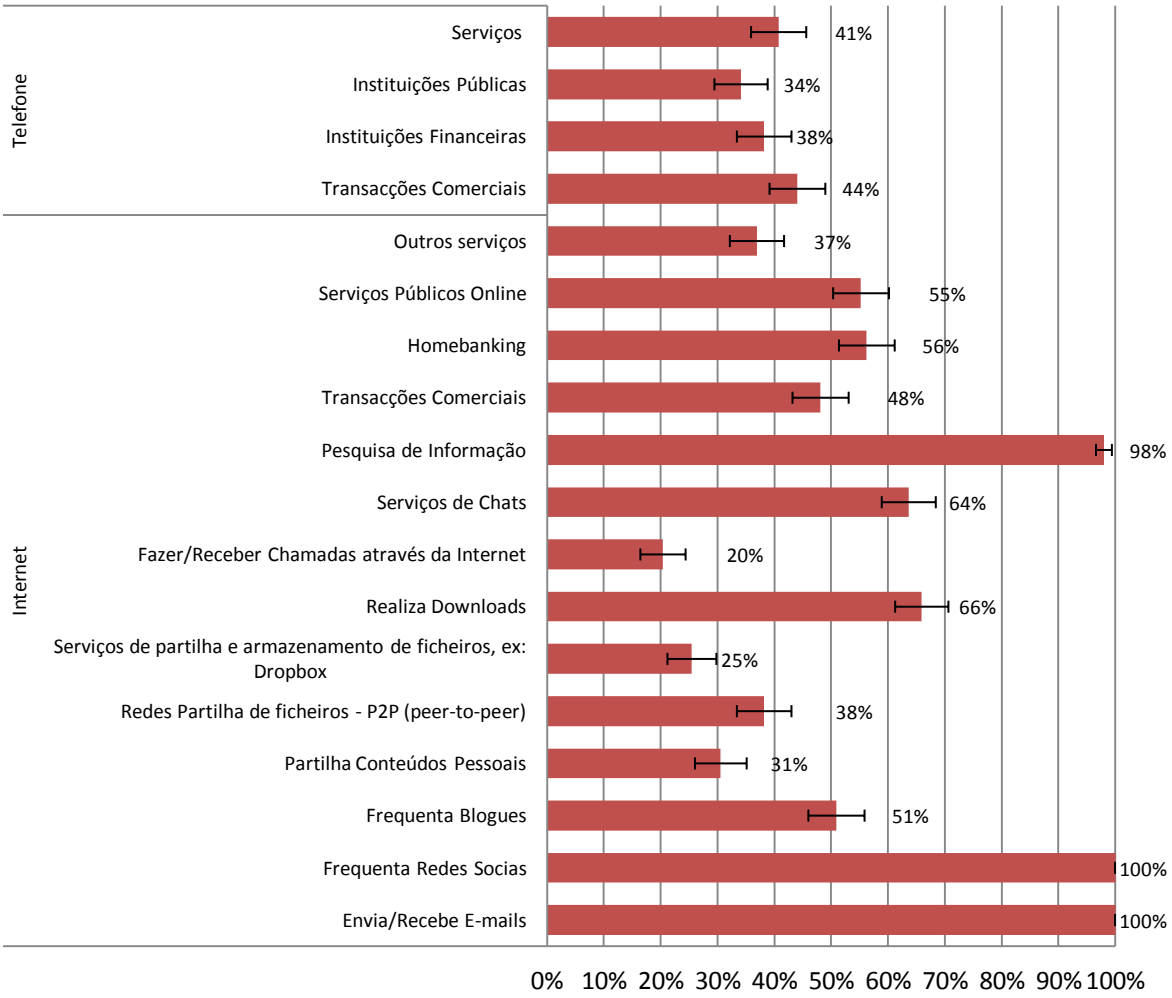

Gráfico 3.21. Respostas obtidas quando questionados quais os serviços que utilizam, com intervalo de confiança de 95%. As margens de erro estão indicadas para cada serviço apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 16)

Num estudo publicado sobre o título "*Sociedade em Rede. A Internet em Portugal 2012"*, mostra-se que, entre as diversas actividades possíveis de serem realizadas através da internet, o envio e recepcção do email é a principal actividade desenvolvida pela maioria dos portugueses, seguida pela utilização das redes sociais e dos serviços de *instant messaging* (Paisana & Lima, 2012).

Os resultados deste estudo vão de encontro com a investigação, onde é possível observar que o envio/recepção de emails, frequência das redes sociais e a pesquisa de informação são as

principais actividades desenvolvidas pela totalidade dos inquiridos, seguido pelos downloads e os serviços de chat.

Na análise do gráfico verifica-se que entre os serviços disponíveis, através da utilização da Internet, o acesso ao banco e aos serviços públicos, as transacções comerciais e os blogues são usados por 50% dos utilizadores.

De acordo com o estudo desenvolvido por (Paisana & Lima, 2012), "*a internet é utilizada por (30,2%) dos inquiridos para adquirir bens ou serviços, (27,5%) recorrem a este meio para reservar ou comprar viagens, (22,8%) usufruem dos serviços de e-banking e (9,6%) fazem compras. No entanto (91,1%) utilizam a internet para procurar noticias, (75,3%) utilizam-na como uma actividade de entretenimento e (74,4%) usam-na para a procura ou verificação de factos*".

Relativamente à utilização das redes sociais, (Paisana & Lima, 2012), revelam também que uma "*percentagem esmagadora dos utilizadores (93,7%) frequentam o facebook. Das funcionalidades disponíveis nas redes sociais, (74,4%) utilizam para o envio de mensagens e (59,7%) o serviço de chat. Na identificação das pessoas com quem os utilizadores estabelecem ligação, (74,0%) declaram que maioritariamente são pessoas de conhecimento pessoal e (26,0%) indicam que estabelecem ligação com pessoas que não conhecem*".

Em relação à utilização dos telemóveis verifica-se que, hoje, os telemóveis são mais do que um simples equipamento de comunicação, tendo-se tornado utilitários indispensáveis para a vida pessoal e profissional. Contudo, à semelhança de qualquer tecnologia, tal como os computadores, tornaram-se vulneráveis a ataques. Pela observação do gráfico, verifica-se que comparativamente com a utilização da Internet como meio de comunicação, o telefone, actualmente, não é o meio preferencial na realização de operações, afirmando menos de metade dos inquiridos usar o telefone no contacto com as instituições financeiras, com os serviços públicos, na realização de transacções comerciais e no contacto com os diversos serviços.
Porém, quase a totalidade dos indivíduos (99,5%) tem um telemóvel (Paisana & Lima, 2012) pelo que tal plataforma de ataque é incontornável.

Com base na informação obtida, conclui-se que, pelo crescimento na utilização da internet e do telefone como meios de comunicação e pela quantidade dos serviços disponibilizados, os engenheiros sociais orientarão os seus ataques na utilização destas plataformas.

3.2.4. As preocupações com segurança na utilização do telefone e da internet.

Na utilização da Internet ou do telefone como meios de comunicação, os utilizadores poderão ser vítimas de diversos tipos de ataque de engenharia social, abordados no capítulo I.

Quando questionados sobre a preocupação com segurança quando realizam operações através do telefone ou da internet, a maioria, como é possível observar pelo gráfico, preocupa-se mais com a segurança na utilização da internet.

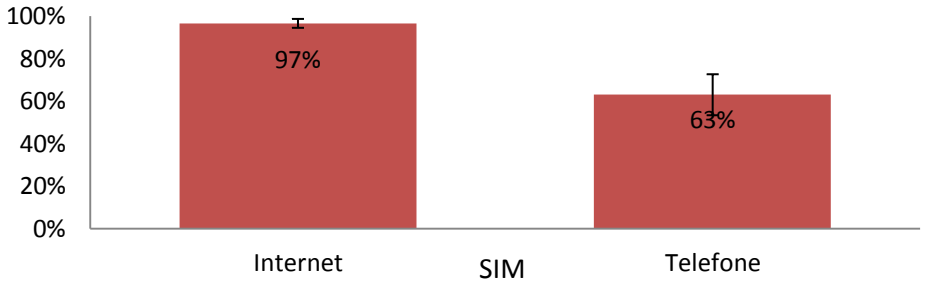

Gráfico 3.22. Resultado das respostas dadas quando questionados se quando realizam operações através do telefone/internet se preocupam com a segurança, com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 17)

3.2.5. As medidas de segurança aplicadas

No gráfico 24 apresentam-se os resultados relativos ao nível de aplicação das medidas de segurança.

Os dados obtidos serão analisados através da utilização de gráficos, tentando-se verificar a existência de alguma relação entre o tipo de medidas com a idade dos utilizadores. Os resultados permitirão identificar quais as principais medidas de segurança que são aplicadas.

A informação é um importante activo, para as pessoas e para as organizações, que necessita de ser protegida. Nesse sentido é necessário que sejam desenvolvidos e implementados um conjunto de procedimentos ou medidas, que possam garantir a confidencialidade, integridade e a disponibilidade da informação. Os procedimentos ou as medidas, independentemente dos objectivos, deverão ser aplicadas como forma de prevenção ou de protecção.

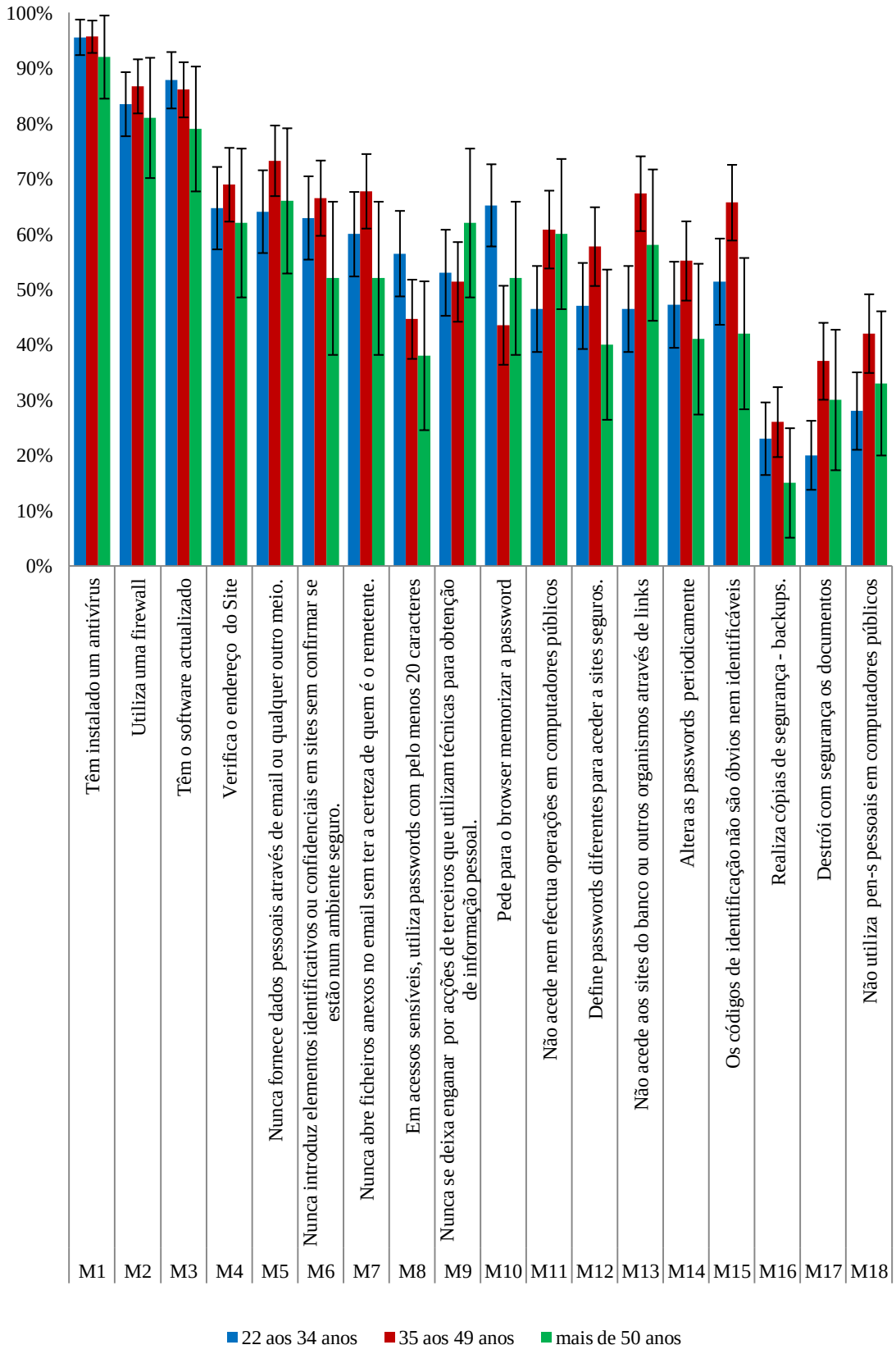

Gráfico 3.23. respostas obtidas com base na faixa etária, quando questionados sobre quais os cuidados que adoptam quando navegam na internet, com intervalo de confiança de 95%. As margens de erro estão indicadas para cada medida apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 18)

Pela análise do gráfico é possível observar as seguintes realidades:

- Upsides - as seguintes medidas são aplicadas por mais de 70% dos utilizadores:
  - *Têm instalado um antivírus*;
  - *Utilizam uma firewall; e*
  - *Têm o software actualizado*

- Downsides – as seguintes medidas são executadas por apenas 30% dos utilizadores:
  - *Realiza cópias de segurança – backups*;
  - *Destrói com segurança os documentos*;
  - *Não utiliza pen-s pessoais em computadores públicos* são executadas.

Em relação à aplicação das medidas M8 e M9, (40%) afirmaram executá-la. A medida M8 – *Em acessos sensíveis, utilizam passwords com pelo menos 20 caracteres* não é de fácil utlização, podendo a sua aplicação ter um resultado diferente do seu objectivo inicial.

A medida M10 não pode ser considerada como um procedimento de segurança, uma vez que existem aplicações distribuídas na internet que permitem obter a informação armazenada no *browser*. Foi entre os utilizadores com idades entre os 22 e os 34 anos os que mais afirmaram executar este tipo de medida.

Na identificação do nível de aplicação das medidas de segurança, constatou-se que os utilizadores com mais de 50 anos foram os que demonstraram uma menor execução das medidas. Foi nesta faixa que mais indicaram - *Nunca se deixa enganar por acções de terceiros que utilizam técnicas para obtenção de informação pessoal.*

Com o objectivo de se identificar a origem do software antivírus que utilizam, uma vez que a medida é referenciada por 94% dos inquiridos, os utilizadores foram questionados acerca de tal.

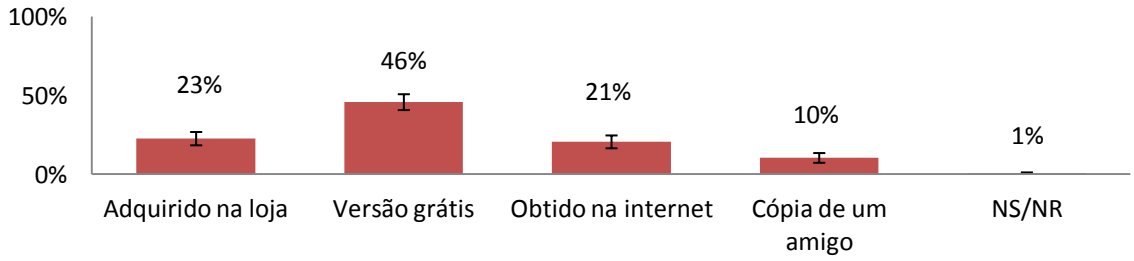

Gráfico 3.24.Resultado das respostas dadas quando questionados para indicar qual a proveniência do antivírus que têm instalado no computador, com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 19)

Através da análise do gráfico é possível observar que a versão de antivírus mais utilizada é a versão grátis. A utilização de um software não legítimo poderá comprometer a garantia da confidencialidade, integridade e disponibilidade da informação. Na execução de um *software* "pirateado", *interesting software*, o utilizador poderá estar a instalar um *spyware*, comprometendo dessa forma a segurança da informação.

3.2.6. O nível de conhecimento sobre a engenharia social

Quando questionados sobre se já ouviram falar em ataques de engenharia social, (55%) responderam positivamente.

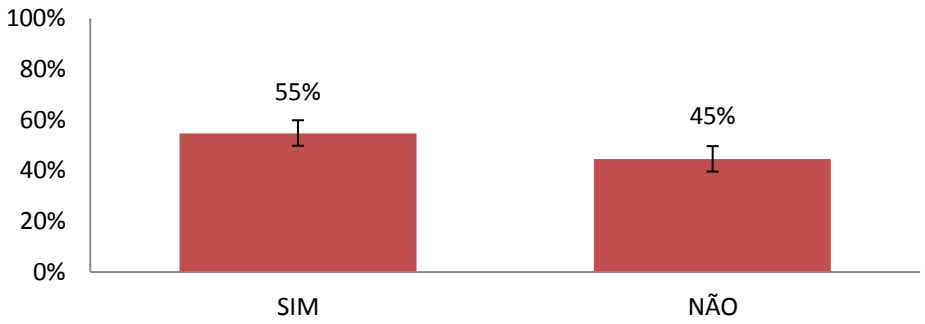

Gráfico 3.25.Resultado das respostas quando questionados se já ouviram falar em ataques de engenharia social, com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 20)

Os resultados obtidos são preocupantes, tendo em atenção que a amostra é constituída por indivíduos com um maior acesso à informação. É possível, portanto, afirmar-se que os resultados demonstram que a engenharia social ainda é um assunto pouco abordado.

Na análise das questões seguintes teremos apenas, em conta as respostas dos que já ouviram falar em ataques de engenharia social, ficando dessa forma a amostra reduzida a 216 indivíduos.

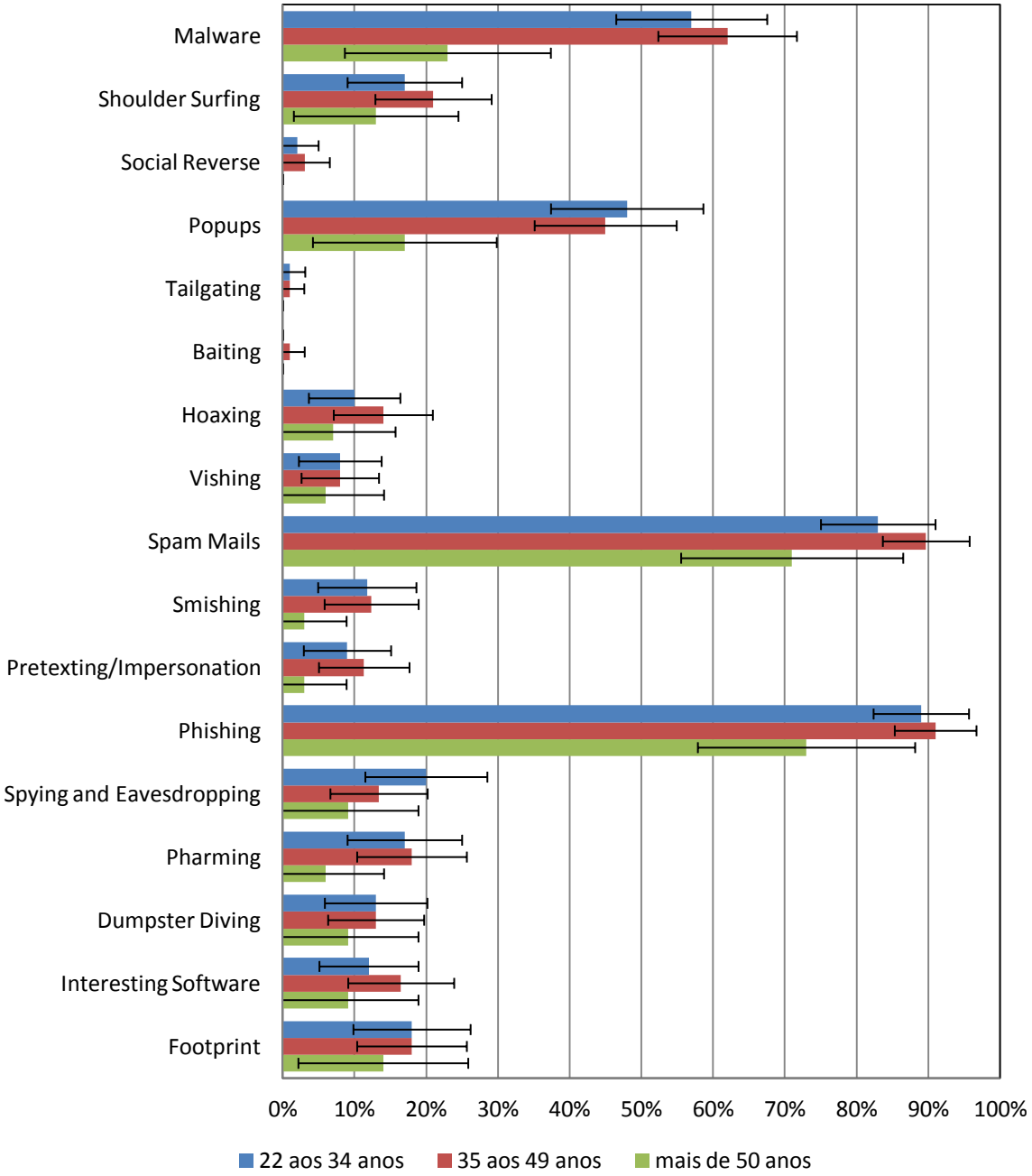

Gráfico 3.26.Resultado das respostas, de acordo com a faixa etária, sobre as técnicas de ataque mais conhecidas, com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 21)

As técnicas de ataque de engenharia social mais conhecidas são claramente o *Phishing* e o *Spam-mails*, seguidas pelas técnicas de *Malware* e *Pop-ups*. Relativamente às restantes técnicas os valores são pouco significativos, representando o nível de desconhecimento dos utilizadores sobre estas.

Na análise dos dados, com base na faixa etária, verifica-se que os utilizadores com mais de 50 anos são os que demonstram um menor conhecimento sobre as técnicas de ataque de engenharia social.

3.2.7. As técnicas de ataque mais utilizadas

Com o objectivo de se identificar o número de vítimas de ataque de engenharia social, quando questionados, (40%) dos inquiridos indicaram terem sido vítimas e (38%) não aceitaram responder à questão.

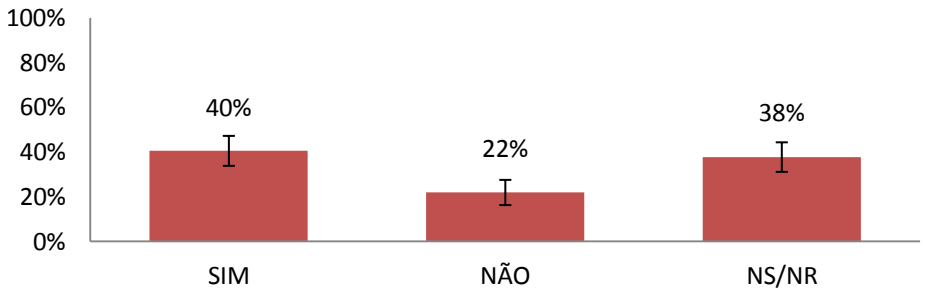

Gráfico 3.27.Resultados das respostas quando questionados se foram alvo de alvo de um ataque de engenharia social, com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 22)

Relativamente aos que responderam NÃO ou aos que não aceitaram responder, nada garante não terem sido vítimas de ataque, dado que por vezes os ataques de engenharia social são de difícil detecção.

Na análise das questões seguintes, a amostra fica reduzida a (n=87) uma vez que só se contabilizam os que afirmaram terem sido vítimas de ataque de engenharia social.

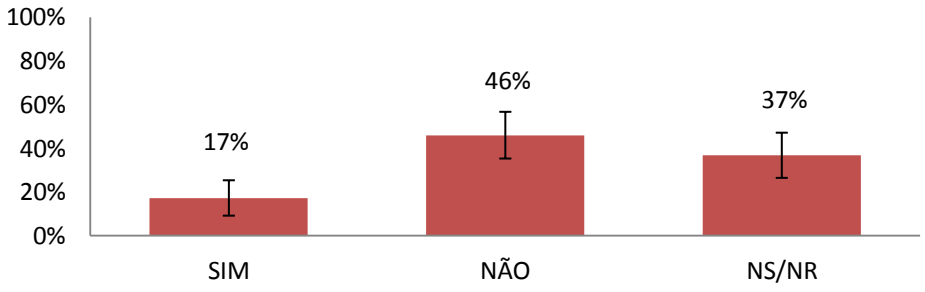

Gráfico 3.28.Resultados das respostas quando questionados se o ataque de que foram alvo foi bem sucedido, com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 23)

Dos inquiridos que foram vítimas de ataque de engenharia social, (17%) afirmou que o ataque foi bem-sucedido. Relativamente aos que responderam NÃO ou que não aceitaram responder, o medo poderá ser a principal razão porque poderão estar a demonstrar que são vulneráveis a um possível ataque.

Os *spams* e o *phishing*, entre as diversas técnicas, são as mais utilizadas nos ataques de engenharia social. Os valores obtidos, em relação às restantes técnicas, são pouco significativos. Tal poderá dever-se, com bastante possibilidade, ao facto de serem as técnicas mais conhecidas e não as que efectivamente resultaram.

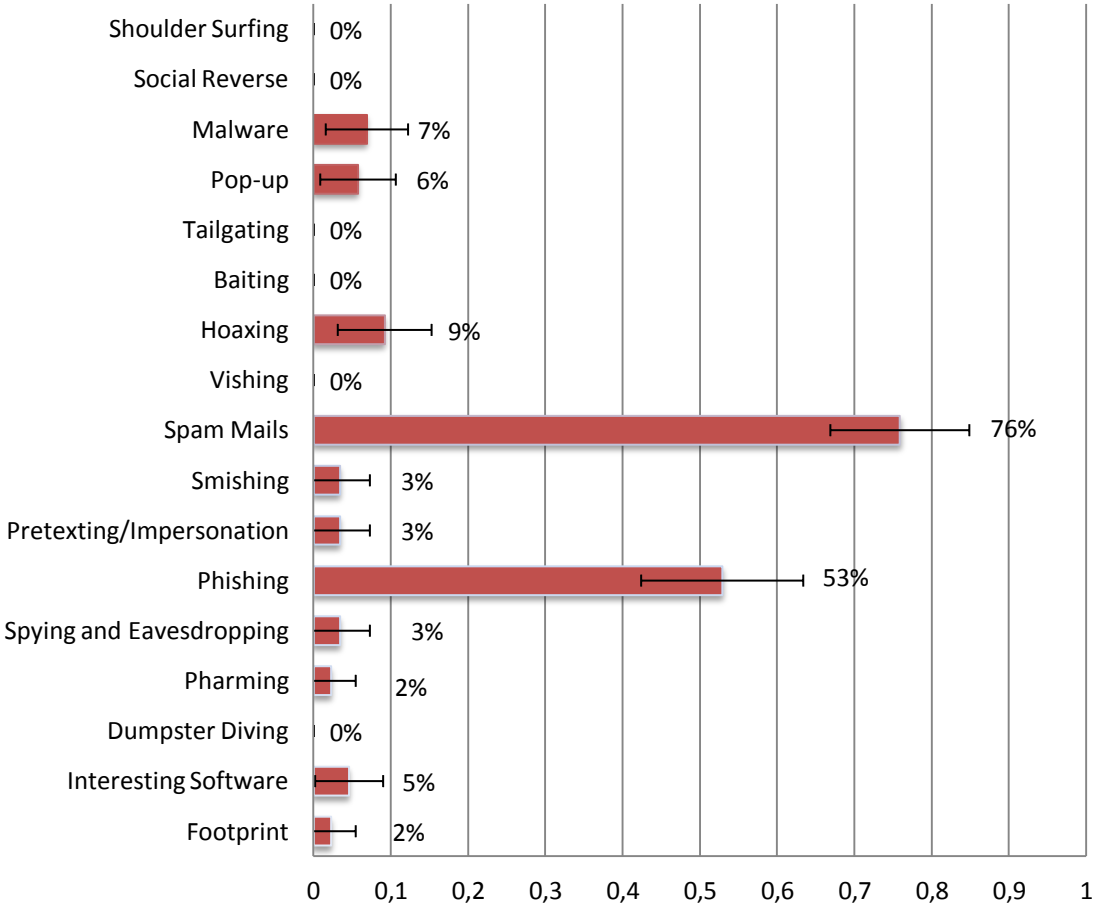

Gráfico 3.29.Resultado das respostas quando questionados para identificar o tipo de ataque de que foram alvo, com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 24)

A reduzida capacidade demonstrada, pelos utilizadores, na identificação das técnicas de ataque que poderão ter sido alvo, está relacionada com o nível de conhecimento. A formação tem um papel importante na segurança de informação.

3.2.8. A principal motivação dos ataques

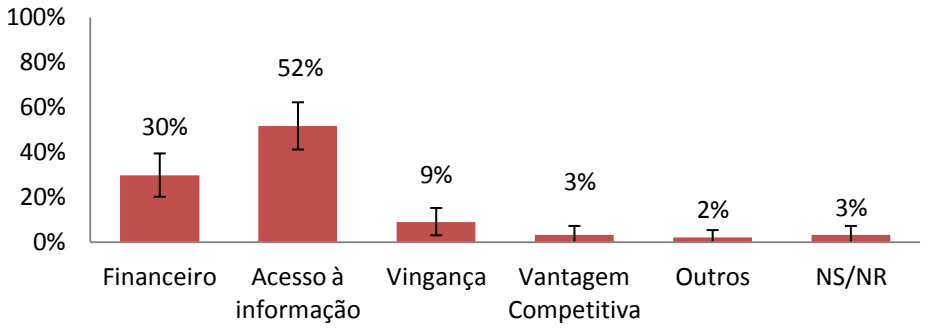

Gráfico 3.30.Resultado das respostas quando questionados para identificar qual o motivo do ataque, com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 25)

Com base nos dados, verifica-se que o acesso à informação (52%) é o principal motivo dos ataques, seguido por motivos financeiros.

3.2.9. A participação dos ataques

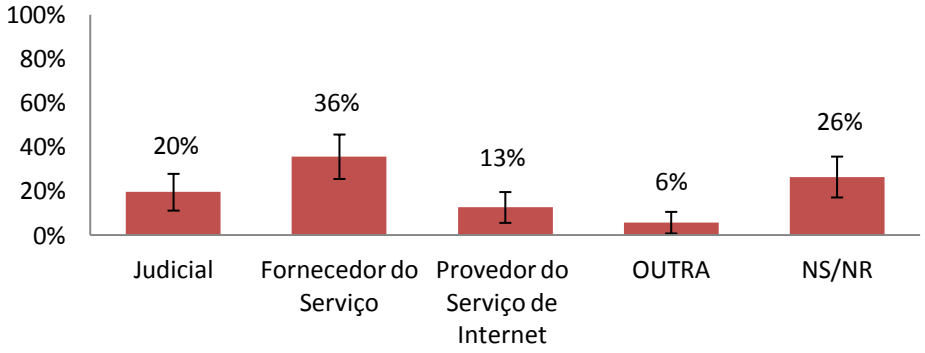

Gráfico 3.31.Resultado das respostas quando questionados para identificarem a entidade onde participaram o ataque de que foram alvo, com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 26)

Quando questionados sobre a identificação a que entidades participaram o ataque de que foram alvo, a maioria, indicou ter participado ao fornecedor do serviço enquanto (26%) não aceitaram responder à questão.

3.2.10. Identificação das plataformas de ataque.

O engenheiro social, no desenvolvimento de um ataque, poderá necessitar de utilizar um meio de comunicação como forma de estabelecer contacto com a vítima. Quando questionados sobre

qual a plataforma usada no ataque de que foram alvo, a maioria indicou o email (45%), seguido pelas páginas web (22%) e as redes sociais (15%).

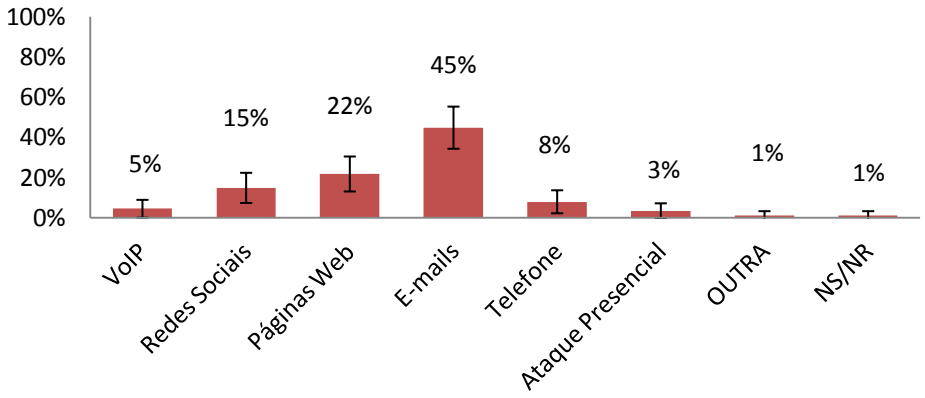

Gráfico 3.32. Resultado das respostas quando questionados para identificar qual a plataforma de ataque usada, com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 27)

Com base nos resultados obtidos, relativamente às técnicas e às plataformas de ataque mais utilizadas, pode-se concluir que a Internet é o meio preferencial na realização dos ataques, sendo todos os demais valores pouco significativos.

3.2.11. O sentimento em relação aos riscos de segurança no futuro.

Quando questionados para identificar no futuro quais serão as plataformas de ataque mais utilizadas, a maioria indicou as redes sociais, seguidas pelo email.

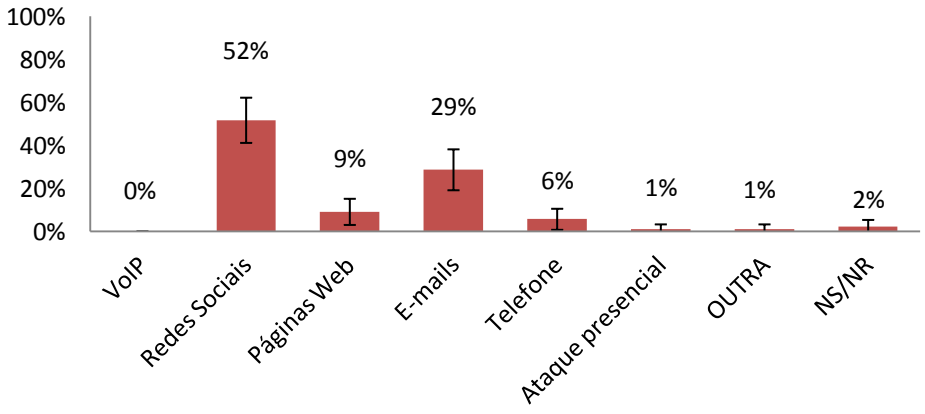

Gráfico 3.33. Resultado das respostas quando questionados para identificar no futuro quais serão as plataformas de ataque mais utilizadas, com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 28)

Em relação ao sentimento sobre os riscos de segurança no futuro, (52%) dos inquiridos pensam que continuarão a piorar.

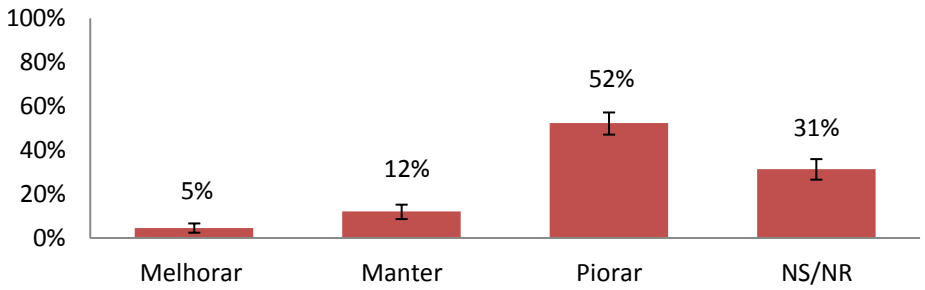

Gráfico 3.34.Resultado das respostas quando questionados para identificarem qual o sentimento em relação aos riscos de segurança no futuro, com intervalo de confiança de 95%. As margens de erro estão indicadas apenas graficamente, valores omitidos por razões de legibilidade (para os valores exactos, ver Anexo III, tabela 29)

CAPÍTULO IV – DEFINIÇÃO DE UMA TAXONOMIA DE BASE

Neste capítulo será proposta uma nova classificação dos ataques de engenharia social com base no tipo de abordagem e na forma de contacto entre o engenheiro social e a vítima.

Para a validação da proposta serão usados diversos exemplos em diferentes cenários que serão analisados com base na classificação proposta e na classificação de Peltier. No desenvolvimento da investigação será, também, identificada a relação existente entre as diferentes técnicas de ataque e a identificação da relação entre as técnicas e as ameaças.

4.1. INTRODUÇÃO

Hoje, as instituições no decorrer do desenvolvimento das suas actividades, numa sociedade em constante competição, disponibilizam serviços, de forma a responderem às necessidades dos seus clientes e colaboradores, através da utilização dos diferentes meios e plataformas de comunicação.

A engenharia social, actualmente, é um dos principais desafios da segurança. Anteriormente, o principal problema estava relacionado com a implementação de medidas de segurança física para protecção dos sistemas de informação contra os acessos não autorizados. Com a crescente dificuldade em ultrapassarem as barreiras tecnológicas, o ser humano tornou-se o principal alvo de ataque.

Os engenheiros sociais através da utilização de um conjunto de técnicas de engenharia social, necessários para a concretização dos seus objectivos, usam os diferentes meios e serviços como plataformas para o estabelecimento de contacto com as suas vítimas e para concretizarem os seus ataques.

As classificações de ataque apresentadas, pelos diversos autores abordadas no estado da arte, não respondem às dificuldades encontradas, por exemplo, algumas das técnicas consideradas como de base-humana poderão, também, ser desenvolvidas através da utilização dos meios tecnológicos, classificando-as dessa forma como ataques de base-técnica. Com o intuito de auxiliar no desenvolvimento das políticas de segurança, a classificação proposta observa, na sua análise, o tipo de abordagem, o meio de comunicação e a plataforma de ataque.

4.2. DEFINIÇÃO DA TAXONOMIA DE BASE

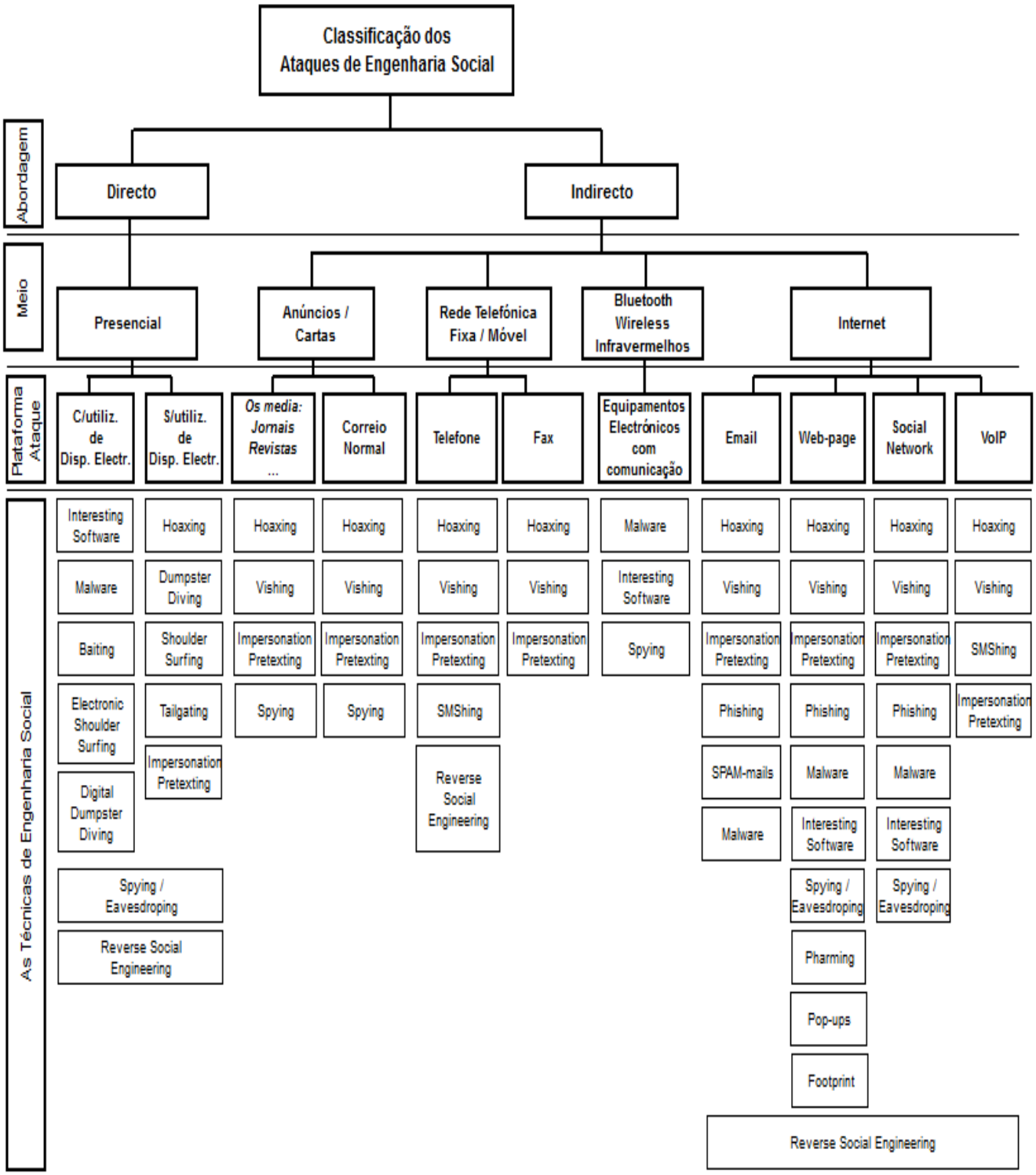

Figura 4.7. Classificação proposta dos ataques de engenharia social.

Peltier (2006), entre os diversos autores abordados no estado de arte, classifica os ataques de engenharia social em ataques de base humana vs. de base técnica. Os ataques de base humana são definidas como "*human based refers to a person-to-person interaction used to obtain the*

desired action" e os de base técnica "*technology based means having an electronic interface to attempt to achieve the desired outcome*".

A classificação proposta é baseada numa estrutura constituída por três níveis:

- Primeiro nível – identificação do tipo de abordagem;
- Segundo nível – identificação dos meios de comunicação;
- Terceiro nível – identificação das plataformas de ataque.

Na identificação do tipo de abordagem é tido em conta a forma de contacto explorado pelo engenheiro social, podendo este ser *directo* ou *indirecto*. No contacto directo não existe a necessidade de utilização de nenhum meio de comunicação, telefone ou internet, para o estabelecimento de ligação entre a vítima e o engenheiro social. O contacto é realizado *in loco*, no local, próximo da vítima, podendo ser executado pelo próprio ou com o recurso a dispositivos electrónicos, entre eles, câmaras de filmar, máquinas fotográficas, microfones, binóculos, etc. Estes equipamentos são muito utilizados nas técnicas de espionagem.

O contacto indirecto é caracterizado pela utilização da rede internet, da rede telefónica fixa/móvel, correio normal e o recurso aos *media* para o estabelecimento de contacto com a vítima. Neste tipo de abordagem também estão incluídos os contactos estabelecidos pela utilização da tecnologia *bluetooth*, *infravermelhos* e *wireless*. O risco do engenheiro social ser identificado neste tipo de contacto é menor por não existir uma proximidade com a vítima, sendo esse um dos motivos da sua maior utilização.

Na identificação das plataformas são referenciadas as vias de ataque, isto é, os meios e os serviços através dos quais os ataques são realizados.

Na referência à utilização da rede telefónica fixa/móvel não se incluí o acesso ao serviço de internet, referindo-se, apenas, à normal utilização dos equipamentos telefónicos e equipamentos de fax. O fax é um tipo de equipamento usado pelas empresas/instituições na execução da suas actividades e através do quais podem ser desenvolvidos ataques. Um engenheiro social fazendo-se passar por uma outra pessoa, aplicando a técnica de *Impersonation/Pretexting*, envia um fax para uma instituição financeira a pedir que sejam alterados os dados pessoais referentes à vítima, morada, contacto telefónico, NIB etc.

Os telefones e os telemóveis tornaram-se num equipamento essencial no dia-a-dia no desenvolvimento das relações pessoais e profissionais. Com base nos dados publicados pela PORDATA, em Portugal, o número de assinantes do serviço telefónico aumentou em 100%

entre 2001 e 2011, representando agora os dezasseis milhões, significando que cada Português possui na média 1,6 telemóveis. Através da sua utilização como plataforma de ataque podem ser aplicadas as técnicas *SMShing*, *Impersonnation*, *Hoaxing*, *Vishing* e *Reverse Social, etc.* A título ilustrativo, um engenheiro social "*smisha*" uma vítima através do envio de uma mensagem SMS fraudulenta, solicitando-lhe que faça algo qu em princípio não faria.

Na utilização dos *media* como plataforma de ataque, o engenheiro social consegue potencialmente atingir dois objectivos: a) chegar a um maior número de pessoas e b) credibilizar a informação. A utilização de um jornal de referência para a colocação de um anúncio dará uma maior credibilidade.

Illustrativamente, o engenheiro social poderá colocar um anúncio de uma oferta de emprego com o objectivo de obter informações sobre o alvo de ataque, num jornal de referência, de forma a captar o interesse de ex-trabalhadores da empresa que pretende atacar. O candidato ao emprego, magoado com a empresa com quem tinha trabalhado torna-se uma boa fonte de informação.

O correio é uma outra fonte, rica, de informação e pela sua observação o engenheiro social consegue obter informação necessária para a realização de um ataque, por exemplo, o *impersonation/Pretexting*.

O *bluetooth*, infravermelhos e *wireless* são um conjunto de tecnologias que estão disponíveis nos mais diversos tipos de equipamentos, telemóveis, portáteis, tablets, etc. A sua utilização permite o estabelecimento de ligação entre os diversos tipos de equipamentos. A falta de informação dos utilizadores sobre o modo de funcionamento destas tecnologias, torna-os vulneráveis a diversos tipos de ataque, tais como, a instalação de *spywares* como forma de obtenção de informação.

A utilização da internet como meio de comunicação, principalmente, nas empresas, está em forte crescimento. De acordo com a PORDATA, a realidade portuguesa é a seguinte:

1. em 2012, a taxa de utilização da internet, pelas empresas com 10 e mais pessoas ao serviço, é de 95%;
2. no ano 2011 o número de assinantes do serviço de internet rondava os dois milhões, tendo desde 2001 até ao presente aumentado 600%.

Com base na investigação desenvolvida constatou-se que a Internet é o principal meio utilizado no estabelecimento de contacto com as instituições financeiras e com os organismos públicos e é o meio preferencial na realização de ataques de engenharia social.

As técnicas de ataque mais utilizadas, *Phishing* e o *spam mails*, utilizam este meio de comunicação.

Na classificação proposta, ao se fazer referência à internet como meio de comunicação, inclui-se a utilização de todo o tipo de equipamentos que permita o acesso à internet, nomeadamente telemóveis de última geração, *smartphones*, computadores, tablets, etc.

A internet como meio de comunicação permite o acesso a uma variedade de serviços, redes sociais, email, páginas web, chamadas telefónicas etc. Através do gráfico 4 é possível observar alguns dos serviços disponíveis na utilização deste meio.

Na referência às redes socias como plataformas, incluem-se as redes de partilha de ficheiro *P2P* (*peer-to-peer*), *Facebook*, *Twiter*, *Myspace*, *Msn*, *Linkelin*, etc. As redes sociais pelas suas características são redes que permitem o estabelecimento de relações pessoais e profissionais. Estas plataformas poderão ser usadas para a obtenção de informação e para a realização dos ataques. Na utilização destas redes, as pessoas disponibilizam a sua informação pessoal e profissional que poderá ser usada no desenvolvimento de um ataque. Tendo em conta a facilidade de criação de uma conta, um indivíduo, através da utilização de fotografias disponíveis na internet, poderá criar uma página com dados falsos de forma a estabelecer um contacto ou relacionamento com um determinado grupo ou pessoa.

De acordo com os dados obtidos na nossa investigação, sobre quais serão no futuro as plataformas de ataque mais utilizadas, a maioria dos inquiridos indicaram as redes sociais.

Efetivamente, é crescente a utilização pelos engenheiros sociais dos diversos serviços disponíveis - *chat,* o envio de mensagens, criação de álbuns fotográficos, jogar e a procura de amigos – que podem servir como plataformas de ataque. O *impersonation/pretexting*, *hoaxing*, *spying*, *malware* e *interesting software* são alguns dos exemplos das diversas técnicas de ataque possíveis de serem executadas.

Na definição das páginas web como plataformas de ataque, estão inseridos os blogues, os *sites* de partilha de vídeo, downloads, técnicos, informativos, etc. Na utilização destas plataformas podem ser aplicadas as técnicas *phishing*, *Impersonation/*Pretexting, *Malware*, *Software*

Interesting, footprint, pharming, Pop-ups, Spying, social reverse, etc. Por exemplo, na utilização dos *sites* especializados ou blogues, o engenheiro social, fazendo-se passar por um especialista numa determinada área, através da utilização de informação falsa, aconselha os visitantes a executar um conjunto de acções que os poderão colocar vulneráveis a um ataque. Actualmente, está na "moda" a utilização de petições *online*, sendo possível através deste tipo de serviços obter um conjunto de informações diversa como, e.g. o nome, número de telefone, número de contribuinte ou o número de identificação pessoal dos indivíduos.

Por fim, na utilização da tecnologia VoIP (Voice over Internet Protocol) o contacto telefónico é estabelecido através da rede internet. O engenheiro social, recorrendo a esta tecnologia, consegue aplicar técnicas idênticas às usadas através da rede telefónica convencional. Em Portugal ainda não é possível possuir um número de telefone, dificultando a identificação do número de origem da chamada através do endereço IP.

No desenvolvimento das políticas de segurança é importante que os responsáveis tenham a capacidade de identificar e compreender a relação existente entre as diferentes técnicas. Tal compreensão permitirá o desenvolvimento de medidas e a implementação de mecanismos que permitam reduzir o risco de um ataque bem-sucedido.

Na aplicação de uma técnica de engenharia social, identificada como ténica principal, o engenheiro social poderá necessitar de recorrer a um conjunto de outras técnicas, definidas como complementares.

Por exemplo, para a execução de um ataque do tipo *vishing*, o engenheiro social poderá recorrer à aplicação da técnica *SMShing*, no envio de uma mensagem SMS, para solicitar à vítima que estabeleça um contacto telefónico.

Quadro 4.1. Identificação da relação entre as técnicas.

Técnica a aplicar	Técnica Complementar: Hoaxing	Dumpster Diving	Shoulder Surfing	Digital Dumpster Diving	Tailgating	Spying and Eavesdroping	Reverse Social or Quid pro quo	Impersonation / Pretexting	Baiting	Smishing	Vishing	Software Interesting	Phishing	SPAM-mails	Footprint	Pharming	Malware
Hoaxing		X	X	X		X											
Shoulder Surfing	X						X	X									
Digital Dumpster Diving	X		X		X	X	X	X									
Tailgating	X	X	X			X		X									
Spying and Eavesdroping	X	X	X	X	X		X	X	X	X	X	X	X		X		X
Reverse Social or Quid pro quo	X	X	X	X		X		X	X			X		X	X		X
Impersonation / Pretexting	X	X	X	X		X			X				X				X
Baiting	X																
Smishing	X							X									
Vishing	X							X		X			X				
Software Interesting	X								X	X				X			
Phishing	X							X		X	X			X		X	
SPAM-mails	X							X									
Pharming										X							X
Malware	X							X	X	X		X	X	X			

Para uma melhor compreensão do quadro 4.1, poderá ser necessária a observação do quadro 4.2.

Quadro 4.2 Validação das relações entre as técnicas.

Técnica Aplicar	Técnicas Complementares	Exemplos
Hoaxing	Dumpster Diving Shoulder Surfing Digital Dumpster Diving Spying and Eavesdroping	O engenheiro social na aplicação da técnica *Hoaxing* poderá ter necessidade de recorrer a outras técnicas para a recolha de informação, que permitam identificar o tipo de assunto que poderá ter interesse para a vítima.

Shoulder Surfing	Hoaxing	Para aplicação da técnica *Shoulder Surfing*, o engenheiro social para conseguir aproximar-se da vítima poderá ter necessidade de inventar uma mentira, fazer-se passar por alguém com autoridade ou criar uma situação em que seja necessário recorrer à sua ajuda.
	Reverse Social	
	Impersonation / Pretexting	
Digital Dumpster Diving	Hoaxing	Invenção de uma história que faça com que a vítima permita o acesso ao equipamento.
	Shoulder Surfing	Observação da vítima durante o processo de autenticação
	Tailgating	A técnica deverá ser aplicada para obtenção de acesso ao local.
	Spying and Eavesdroping	Através da observação do lixo digital, o engenheiro social consegue obter a informação.
	Reverse Social	A técnica de engenharia social inversa deverá ser aplicada com o objectivo de a vítima necessitar de ajuda, de tal modo que forneça acesso ao equipamento.
	Impersonation / Pretexting	O engenheiro social poderá fazer-se passar por alguém com autoridade para obter acesso ao equipamento.
Tailgating	Hoaxing	A utilização de uma mentira com o objectivo de obtenção de acesso ao local.
	Dumpster Diving	Para a realização do ataque, o engenheiro social poderá necessitar de obter informação sobre a empresa, tal como a estrutura, o sistema de segurança, colaboradores, etc.
	Shoulder Surfing	
	Spying and Eavesdroping	
	Footprint	
	Impersonation / Pretexting	Fazer-se passar por alguém com autoridade
Spying and Eavesdroping	Hoaxing	A utilização de uma mentira de modo a despertar o interesse da vítima e, dessa forma, estabelecer uma relação de amizade e confiança.
	Dumpster Diving	Métodos de recolha de informação
	Shoulder Surfing	
	Digital Dumpster Diving	
	Tailgating	Obtenção de acesso ao local
	Reverse Social	Criação de uma situação que faça com que a vítima necessite da sua ajuda de modo a obter a sua confiança.
	Impersonation / Pretexting	Fazer-se passar por alguém do interesse da vítima de modo a estabelecer um contacto, uma relação de amizade e obter a sua confiança.
	Baiting	A instalação de um *spyware* para a obtenção de informação
	Smishing	Através do contacto com a vítima por SMS, fazendo-se passar por alguém, tentar obter informação ou fá-la executar algo.
	Vishing	Através do contacto telefónico com a vítima, fazendo-se passar por alguém, tentar obter informação ou persuadir a executar algo.

	Phishing	Envio de um email com um link que leve à instalação de um *spware*
	Interesting Software	Fornecimento de um software do interesse da vítima que permita a instalação de um malware que permita o acesso remoto.
	Footprint	Pesquisa de informação sobre a empresa
	Malware	Instalação de um vírus que permita o controlo remoto.
Reverse Social	Hoaxing	Utilização de uma mentira que faça com a vítima necessite da sua ajuda
	Dumpster Diving	Obtenção de informação sobre os sistemas de informação de modo a identificar as vulnerabilidades da empresa
	Digital Dumpster Diving	
	Spying and Eavesdroping	
	Shoulder Surfing	Obtenção da password de acesso ao sistema
	Impersonation / Pretexting	Fazer-se passar por um especialista ou por alguém com autoridade.
	Baiting	Instalação de um *malware,* através da utilização de uma pen-usb, que crie uma situação em que seja necessário o recurso à sua ajuda.
	Software Interesting	Instalação de um software que crie um problema e seja necessário o recurso à sua ajuda.
	SPAM-mails	Um ataque ao servidor de modo que seja necessário o recurso a um especialista para a resolução do problema
	Footprint	Pesquisa de informação técnica sobre o servidor, de forma a auxiliar o ataque.
	Malware	Instalação de um malware que provoque danos
Impersonation / Pretexting	Hoaxing	Através da utilização de uma mentira, fazer-se passar por alguém com autoridade
	Dumpster Diving	Recolha de informação de forma a credibilizar a sua personificação.
	Digital Dumpster Diving	
	Spying and Eavesdroping	
	Baiting	Instalação de um spyware de forma a obter informação
	Shoulder Surfing	Obtenção dos dados de autenticação, de forma a conseguir fazer-se passar pela vítima.
	Phishing	Através do envio de um email enviado à vitima levá-lo a aceder a um site e a introduzir informação pessoal que depois será utilizada, por exemplo num contacto telefónico com o banco.
	Malware	Propagação de um vírus, por exemplo um *spyware*, com o objectivo de obter informação de forma a ser possível fazer-se passar pela vítima.
Baiting	Hoaxing	Identificação de um dispositivo de forma a despertar o interesse da vítima.
Smishing	Hoaxing	Utilização de uma mentira que cative o interesse da vítima

	Impersonation / Pretexting	Persuasão à execução de uma instrução, fazendo-se passar por alguém ou por uma instituição
Vishing	Hoaxing	Utilização de uma mentira que cative o interesse da vítima
	Impersonation / Pretexting	Fazendo-se passar por alguém ou por uma instituição faz com que a vítima execute a instrução
	Smishing	Através do envio de uma mensagem SMS o engenheiro social solicita à vítima que ligue para um determinado número para um assunto do seu interesse.
	Phishing	Através da utilização de um site "falso" o engenheiro social indica o número para onde os clientes deverão ligar.
Interesting Software	Hoaxing	Através da utilização de uma mentira que leve a vítima a instalar um determinado software.
	Baiting	Identificar uma pen-usb como contendo a última versão de um software do interesse da vítima.
	Smishing	Através do envio de uma mensagem SMS, indica um link onde a vítima poderá adquirir ou actualizar um determinado software.
	SPAM-mails	Envio de emails com a oferta de instalação de um software com grande procura.
Phishing	Hoaxing	Através da utilização de uma mentira que cative o interesse da vítima em aceder a um determinado site "falso".
	Impersonation / Pretexting	No contacto com a vítima fazendo-se passar por alguém ou por instituição induz a vítima a aceder a um determinado site "falso".
	Smishing	Através do envio de uma mensagem SMS solicita a vítima a preencher um formulário alojado num site "falso".
	SPAM-mails	Envio de emails a solicitar que através de um link acedam a um site "falso". e preencha um formulário.
	Vishing	Através de um contacto telefónico solicita à vítima que aceda a um determinado site para actualizar os dados.
SPAM-mails	Hoaxing	Utilização de uma mentira que desperte o interesse da vítima
Malware	Hoaxing	Utilização de uma mentira que desperte o interesse da vítima
	Impersonation / Pretexting	Fazendo-se passar por alguém conhecido ou de confiança recomenda a instalação de um software.
	Baiting	Através da utilização de dispositivos
	Smishing	Envio de uma mensagem SMS com um link para um site que permitirá a instalação de um malware
	Software Interesting	Identificando-se como sendo uma entidade credível fornece gratuitamente uma versão de um software com forte procura.
	Phishing	Através da falsificação dos conteúdos de site conhecido, leva os utilizadores a instalarem o software disponibilizado.

	SPAM-mails	Envio massivo de emails com ficheiros contaminados anexados.

4.2.1. Identificação da relação entre as técnicas e as ameaças.

No quadro 4.3 são apresentadas as principais ameaças que estão associadas à aplicação das técnicas.

Quadro 4.3. Identificação da relação entre as técnicas e as ameaças

Ameaças		Hoaxing A	Dumpster Diving B	Shoulder Surfing C	Digital Dumpster Diving D	Tailgating E	Spying and Eavesdroping F	Reverse Social G	Impersonation / Pretexting H	Baiting I	Smishing J	Vishing L	Software Interesting M	Phishing N	SPAM-mails O	Footprint P	Pharming Q	Malware R
Espionagem	1		X	X	X		X		X							X		X
Roubo de identidade	2		X	X	X			X	X		X	X	X	X		X	X	X
Acesso não autorizado	3	X				X			X									
Propagação de Malwares	4									X	X	X	X	X	X			X
Falsificação de Conteúdos	5										X	X		X			X	
Sobrecarregamento ou Interrupção de Serviço	6					X				X			X		X			X

Na concretização de uma determinada ameaça pode ser necessário o recurso a um conjunto de outras ameaças.

Por exemplo, num ataque de engenharia social inversa em que a ameaça principal é o roubo de identidade, o engenheiro social através da interrupção de um serviço faz com que a vítima necessite de recorrer à sua ajuda.

4.3. VALIDAÇÃO DA PROPOSTA APRESENTADA

A validação da classificação proposta será realizada com base na avaliação da aplicação das técnicas de engenharia social em dois cenários tipo: pessoas e instituições/organizações. Em cada um dos cenários são usados vários exemplos, sendo cada exemplo analisado com base nas

duas classificações: classificação proposta e classificação dos ataques em base-humana e base-técnica. Alguns dos exemplos de um determinado cenário poderão ser usados como exemplo noutro cenário.

Cenário 1: Ataques de engenharia social contra as pessoas.

Exemplo 1.

O engenheiro social através da utilização do email, fazendo-se passar por uma entidade, informa os utilizadores que por questões de segurança é necessário que façam a instalação de um software através do link disponibilizado.

Técnicas Aplicadas	Phishing Hoaxing Interesting Software Malware Impersonation/Pretexting	
	Classificação Proposta	**Classificação Base-Humana e Base-Técnica**
Critérios de Análise	Tipo Abordagem: Indirecto Meios: Internet Plataforma: Email	Ataque de base-humana Ataque de base-técnica

Exemplo 2.

O engenheiro social, através do envio de emails, tenta criar uma rede de solidariedade com o objectivo de apoiar uma causa, por cada email reencaminhado. Por vezes, indicam um NIB e anexam ficheiros contaminados.

Técnicas Aplicadas	Hoaxing Impersonation/Pretexting Malware	
	Classificação Proposta	**Classificação Base-Humana e Base-Técnica**
Critérios de Análise	Tipo Abordagem: Indirecto Meios: Internet Plataforma: Email	Ataque de base-humana Ataques de base-técnica

Exemplo 3.

O engenheiro social, através de um contacto telefónico, fazendo-se passar por representante de uma instituição financeira, solicita à vítima que se identifique.

Técnicas Aplicadas	Hoaxing Impersonation/Pretexting Vishing	
	Classificação Proposta	**Classificação Base-Humana e Base-Técnica**
Critérios de Análise	Tipo Abordagem: Indirecto Meios: Rede Telefónica Plataforma: Telefone	Ataques de base-humana Ataque de base-técnica

Exemplo 4.

A vítima é contactada através de uma mensagem SMS para que ligue para um determinado número de forma a manter o acesso activo ao serviço.

Técnicas Aplicadas	Vishing SMShing Hoaxing; Impersonation/Pretexting	
	Classificação Proposta	**Classificação Base-Humana e Base-Técnica**
Critérios de Análise	Tipo Abordagem: Indirecto Meio: Rede Telefónica Plataforma: Telefone	Ataque de base-técnica Ataques de base-humana

Pela observação dos exemplos 1 e 2 é possível constatarem-se os seguintes elementos:

- a Internet é o meio utilizado para a realização do ataque;
- o engenheiro social, recorrendo ao email como plataforma de ataque, consegue executar um conjunto de técnicas;

- com base na classificação de Peltier, algumas das técnicas seriam classificadas de base humana e outras de base-técnica.
- com a utilização da classificação de Peltier, teriam de ser desenvolvidas políticas de acordo com as características das técnicas utilizadas.
- ao analisarem-se os ataques com base na plataforma utilizada, apenas seria necessária a criação de políticas orientadas na utilização do email como plataforma de ataque.

Nos exemplos 1 e 2, entre as diversas medidas possíveis de serem aplicadas, a utilização de um software antivírus permitiria reduzir a propagação de vírus.

No exemplo 1 seria importante que as instituições nos contactos com os seus clientes utilizassem emails personalizados, com alguns dados de identificação da pessoa em conjunto com a utilização de um código, único por cada cliente, que pudesse garantir a validade da mensagem. Como complemento, as instituições nas suas páginas oficiais, deveriam fazer comunicados sobre as menagens distribuídas.

Identicamente, para os exemplos 3 e 4 são possíveis outras constatações:

- o telefone é usado como plataforma de ataque;
- no desenvolvimento de políticas de segurança, as políticas deverão estar orientadas na utilização do telefone. Por exemplo, na utilização do telefone no estabelecimento de contacto com as instituições, como exemplo as instituições financeiras, por vezes existem falhas de segurança, algumas relacionadas com o processo de autenticação.

O cliente no contacto telefónico com a instituição financeira começa, através de uma chamada automática, por identificar-se inserindo o número do cartão de crédito e o código pessoal. De seguida a chamada é reencaminhada para um operador, independentemente de terem sidos inseridos correctamente os dados de identificação. O cliente é novamente sujeito a um conjunto de perguntas, nome, morada, número de telefone, numero de telefone do local de trabalho, número de identificação pessoal, número de contribuinte e a data de nascimento. É importante referir que no estabelecimento de um novo contacto no mesmo dia ou nos dias seguintes as questões de segurança centram-se nas mesmas.

Na utilização do mesmo tipo de questionário, as instituições colocam em risco a segurança da informação: primeiro, ao serem mantidos o mesmo tipo de perguntas, alguém mal-intencionado depois de obter a informação, no mesmo dia ou no dia seguinte através de uma chamada poderá utilizar essa informação; segundo, numa só chamada, através do questionário, são usados todos os elementos identificativos referentes ao cliente, o que poderá facilitar o trabalho do

engenheiro social na recolha de informação; por fim, o engenheiro social com o conhecimento do tipo de questões usadas, fazendo-se passar por um representante de uma instituição poderá solicitar à vítima que responda ao mesmo tipo de questões. O cliente habituado a responder às perguntas sem questionar o perigo da sua utilização fornece a informação. De acordo com Charles Lively, abordado no capítulo I, o ser humano tem a tendência de reagir de forma mecanizada às situações habituais, agindo dessa forma sem pensar, uma vulnerabilidade que poderá ser explorada pelo engenheiro social na concretização de um ataque.

Os métodos de identificação apresentam falhas que podem comprometer o processo de autenticação. Nos exemplos em que o cliente através da utilização do telefone estabelece contacto com a instituição financeira, seria necessário que no processo de autenticação fossem adoptados um conjunto de procedimentos, tais como, a obrigatoriedade do contacto ser realizado através do número existente no registo do cliente. O processo de identificação deveria ser feito pela utilização dos dados de um cartão matriz. É necessário ter-se em conta que na utilização dos dados pessoais o cliente está a fornecer informação ao operador telefónico, cuja situação laboral por vezes é precária. Os ataques desenvolvidos pelos colaboradores, por vezes, são a maior ameaça à segurança das empresas.

Nos casos em que a própria instituição contacta com o cliente, seria importante que no estabelecimento do contacto o mesmo fosse realizado através de um número único e numa chamada identificada, não anónima, o que permitiria a sua memorização e associação. O representante da instituição deveria identificar-se através da utilização de um código, associado ao cliente, como forma de validar a origem da chamada. Este tipo de procedimento é aplicado pelas empresas de segurança residencial.

Cenário 2: Ataques de engenharia social contra instituições/organizações

Exemplo 1.
Na observação de um anúncio de oferta de emprego, o engenheiro social candidata-se enviando um email com anexos contaminados.

Técnicas Aplicadas	Hoaxing Malware Spying	
	Classificação Proposta	**Classificação Base-Humana e Base-Técnica**

Critérios de Análise	Tipo Abordagem: Indirecto Meios: Internet Plataforma: Email	Ataque de base-humana Ataque de base-técnica

Exemplo 2.

O engenheiro social fazendo parte de uma equipa de suporte circula livremente pela empresa fora das horas de expediente, .

Técnicas Aplicadas	Spying and Eavesdropping Impersonation/Pretexting Support Staff Baiting Malware	
	Classificação Proposta	**Classificação Base-Humana e Base-Técnica**
Critérios de Análise	Tipo Abordagem: Directo Meios: Presencial Plataforma: Sem utilização de dispositivos Eletrónicos;	Ataque de base-humana Ataques de base-técnica

Exemplo 3.

O engenheiro social através da utilização da conversa e da simpatia consegue obter o acesso ao interior da empresa e abandona uma *pen-usb* contaminada.

Técnicas Aplicadas	Hoaxing Tailgating Baiting Malware Spying and Eavesdropping	
	Classificação Proposta	**Classificação Base-Humana e Base-Técnica**
Critérios de Análise	Tipo Abordagem: Directo Meios: Presencial Plataforma: Dispositivos electrónicos	Ataque de base-humana Ataque de base-técnica

Exemplo 4.

Através de pesquisas no lixo o engenheiro social consegue obter informação de forma a fazer-se passar por alguém com autoridade.

Técnicas Aplicadas	Dumpster Diving Hoaxing Impersonation/Pretexting Spying	
	Classificação Proposta	**Classificação Base-Humana e Base-Técnica**
Critérios de Análise	Tipo Abordagem: Directo**,** Indirecto Meios: Presencial,Rede Telefónica Plataforma: S/utilização Disp. Electr; Telefone	Ataques de base-humana

Também de forma idêntica, são possíveis as seguintes constatações para o exemplo 1:

- verifica-se que o email é a plataforma de ataque;
- com base na classificação de Peltier(2006) as técnicas aplicadas são de base-humana.

Através da propagação do *malware* pelo email, o engenheiro social consegue obter informação, *spying*. Na utilização do antivírus seria possível reduzir o risco de ataque.

Nos exemplos 2 e 3 é utilizada a abordagem directa, encontrando-se o engenheiro social presencialmente no local. No exemplo 2, o engenheiro social, fazendo parte de uma equipa de limpeza, consegue circular livremente pela empresa e fora das horas de serviço, observando a informação disponível nas secretárias. Na aplicação da técnica Baiting, o engenheiro social, explorando a curiosidade da vítima, deixa numa secretária uma pen-usb contaminada conseguindo obter o acesso remoto à rede.

Como forma de reduzir o risco originado pela circulação de pessoas "estranhas" dentro das organizações, deveriam ser desenvolvidas políticas, entre elas, a política de secretária limpa, políticas de controlo de acessos e de utilização de dispositivos electrónicos. Estas políticas

terão como objectivo reduzir o risco de acesso a informação não autorizada e de utilização de equipamentos electrónicos, *pen-usb*, máquinas fotográficas, etc.

No exemplo 3, através da exploração das vulnerabilidades do ser humano, abordada no capítulo I, e pela ausência de um controlo de acesso eficiente o engenheiro social consegue obter acesso ao espaço e aplicar um conjunto de técnicas de engenharia social.

A engenharia social, entre as diferentes definições, é definida como a capacidade de enganar as pessoas explorando as vulnerabilidades do ser humano. Pela dificuldade em combater as vulnerabilidades do ser humano, a principal preocupação dos responsáveis pela segurança deveria passar pelo desenvolvimento de um bom plano de formação em conjunto com a implementação de mecanismos eficientes de controlo de acessos. Na implementação de um controlo eficiente seria possível reduzir a possibilidade de execução de um conjunto de técnicas *Tailgating*, *Impersonation/Pretexting*, *Baiting*, *Malware*, *Hoaxing* e *Spying and Eaesdropping*.

No exemplo 4, o engenheiro social explora os dois tipos de abordagem. Primeiro desenvolve um trabalho de pesquisa através da observação do lixo, esta técnica é conhecida como *Dumpster Diving* e foi usada por Kevin Mitnick num dos seus ataques muito conhecido. Depois de obter a informação utiliza o telefone como plataforma de ataque.

Com o objectivo de reduzir a possibilidade de um ataque bem-sucedido, deveriam ser desenvolvidas políticas, pelo menos, para um tipo de abordagem. Ao serem desenvolvidas políticas em relação aos métodos de destruição segura dos documentos, o engenheiro social não conseguiria aplicar a técnica *Dumpster Diving* e dessa forma fazer-se passar por alguém com autoridade. Se a política fosse aplicada na utilização do telefone, essa política deveria passar pela utilização de um código pessoal nos contactos com o responsável TI, o que impediria a aplicação da técnica de *Impersonation/Pretexting*. Através da aplicação das técnicas *Dumpster Diving* e do *Impersonation/Pretexting* , como é possível observar no quadro 3, o engenheiro social consegue executar a técnica de *spying*.

No desenvolvimento de políticas, com base na classificação de Peltier seria necessário a implementação de políticas que fossem ao encontro de cada uma das técnicas utilizadas. Ao serem desenvolvidas políticas na utilização das plataformas e nos meios de comunicação, seria possível reduzir a possibilidade da aplicação de um conjunto de técnicas.

4.4. CONTRIBUIÇÃO DA TAXONOMIA PROPOSTA

As empresas com a necessidade de desenvolverem as suas actividades, e de estarem cada vez mais próximos dos seus colaboradores, parceiros e clientes, recorrem à utilização das diferentes plataformas - telefone, email, redes sociais, web, VoiP, etc.

Na utilização destas plataformas ficam vulneráveis a ataques de engenharia social.

Os responsáveis pela segurança, com o objectivo de reduzirem os riscos de um ataque bem sucedido procuram desenvolver politicas de segurança. A classificação proposta tem por objectivo auxiliar e orientar os responsáveis na forma de como abordar a problemática da engenharia através da:

- classificação dos ataques com base no tipo de abordagem
- identificação das técnicas e das plataformas de ataque
- identificação da relação de dependência entre as técnicas
- identificação das ameaças resultantes da aplicação das técnicas
- redução dos custos na implementação das políticas

CAPÍTULO V – CONCLUSÕES

5.1. DISCUSSÃO

A investigação foi dividida em três etapas. Na primeira etapa fez-se uma introdução teórica sobre a engenharia social através da análise das vulnerabilidades do ser humano e das diferentes técnicas de ataque; na etapa seguinte desenvolveu-se uma investigação com o objetivo de obtenção de respostas sobre as diversas questões relacionadas com a segurança da informação; por último foi proposta uma classificação dos ataques de engenharia social, com base no tipo de abordagem.

No estudo desenvolvido limitou-se a investigação às técnicas consideradas mais relevantes. Algumas pelas suas semelhanças não foram referenciadas. Na observação das vulnerabilidades exploradas pelo engenheiro social, baseou-se a investigação nos factores de influência abordados por Cialdini e nos vectores de ataque relatados por Charles Lively, assuntos abordados no capítulo I no ponto 1.2. Os trabalhos desenvolvidos por ambos autores são referenciados em diversas investigações.

Na segunda etapa da investigação teve-se por objectivo, entre outros, identificar os principais serviços utilizados através da internet e do telefone, o nível de conhecimento sobre a engenharia social, os principais alvos e objectivos dos ataques, a atitude de segurança e as técnicas de ataque mais usadas. Alguma da informação obtida poderá ser útil no desenvolvimento das políticas de segurança, uma vez que permitem obter uma imagem da realidade portuguesa sobre a problemática da segurança.

Na análise dos resultados do inquérito aos responsáveis TI, constatou-se que apenas 44% possuem habilitação relacionada com as tecnologias de informação. Este dado poderá servir para justificar alguns dos resultados obtidos, relativamente ao nível de conhecimento sobre as técnicas de ataque e às medidas de segurança.

Na identificação das técnicas de ataque mais conhecidas e mais utilizadas, a maioria dos utilizadores e dos responsáveis TI indicaram o *phishing* e os *Spam-mails*. Ambas as técnicas utilizam a internet como meio de comunicação e o email como plataforma de ataque. Os resultados foram pouco significativos em relação às restantes técnicas.

Em relação às medidas de segurança, verificou-se que a instalação do antivírus e a utilização de uma firewall são as medidas mais aplicadas. Na referência à instalação do antivírus, existiu a necessidade de identificar a proveniência do software, uma vez que a utilização de um software não genuíno pode colocar em risco a segurança.

Na identificação das medidas de segurança, foram utilizadas algumas questões "rasteira" com o objectivo de validar a credibilidade das respostas e a capacidade dos inquiridos para distinguirem as medidas seguras das não seguras:

- (44%) dos responsáveis TI e (55%) dos utilizadores afirmaram *"Nunca se deixa enganar por acções de terceiros que utilizam técnicas para obtenção de informação"*. Ao ser feita esta afirmação os inquiridos demonstraram um total desconhecimento sobre as características das técnicas de engenharia social. As técnicas de ataque de engenharia social, ao contrário dos ataques técnicos, exploram as vulnerabilidades do ser humano, entre elas, as emoções, a inocência e o desconhecimento. Comparativamente em relação aos ataques técnicos, em que é possível a implementação de barreiras de segurança, sobre as vulnerabilidades do ser humano não é possível a implementação de mecanismos de controlo.

- (16%) dos responsáveis TI e (46%) dos utilizadores afirmaram que "*Em acesso sensíveis utilizam passwords com pelo menos 20 caracteres* ". A afirmação da aplicação desta medida é de duvidosa credibilidade e fiabilidade. O que nos poderá levar a pensar que é possível que as outras respostas estejam exageradas no sentido de transmitirem uma ideia de segurança superior ao que realmente existe, o que sugere que os restantes resultados devem ser analisados de uma forma conservadora, isto é, o valor real das respostas dadas deverá ser inferior ao que os inquiridos indicaram. Na utilização de uma password desta dimensão o utilizador com o objectivo de facilitar a sua memorização poderá ter que fazer uso de informação pessoal na construção da password, por exemplo, utilização de um conjunto de dados relativos ao nome, data de nascimento, número de contribuinte, número de telemóvel. Na dificuldade de memorização poderá ter que anotar a password em algum local ou permitir a sua memorização através da utilização de aplicações. A utilização de uma password desta dimensão poderá ter um efeito contrário aos objectivos da sua aplicação.

- (22%) dos responsáveis TI e (54%) indicaram que "*Pede para o browser memorizar a password"* . Este acto não poderá ser considerado como uma medida de segurança, porque existem imensas aplicações na internet que permitem a leitura das passwords memorizadas.

A preocupação com a formação não é a principal prioridade das empresas, apenas (23%) desenvolvem acções de formação. A formação tem uma importante função na prevenção contra os ataques de engenharia social, no sentido em que permite promover a consciencialização das pessoas em relação aos riscos e às atitudes de segurança. Através da consciencialização das pessoas do valor da informação, é possível evitar que alguns riscos, tais como fornecer informações por telefone ou deixar papéis na impressora com informações acessíveis.

No preenchimento do inquérito os inquiridos foram solicitados a disponibilizar o endereço de correio eletrónico. Foi entre os inquiridos do sexo feminino e com mais de 50 anos os que mais disponibilizaram. Por questões de segurança este facto é importante, com base nos dados obtidos do inquérito, o email é o meio preferencial dos engenheiros sociais no desenvolvimento de um ataque.

Com a multiplicidade de plataformas de comunicação, resultado da evolução das tecnologias, tornam o processo de prevenção e da mitigação dos riscos cada vez mais difícil. No capítulo IV, foi proposta uma nova classificação dos ataques de engenharia social com base no tipo de abordagem. Os resultados obtidos na fase de inquérito contribuíram para a identificação das características dos ataques.

Através da classificação proposta, as preocupações com a segurança deixarão de estar orientadas para as características das técnicas e centrar-se-ão nas plataformas e nos serviços utilizados de forma a melhorar a consciencialização dos utilizadores nos riscos da utilização das diferentes plataformas, uma vez que estes são os meios de ligação entre o atacante e a vítima.

Relativamente à comparação entre a abordagem proposta nesta tese e a proposta por Peltier, a mais comummente – e quase universalmente – referenciada por outros autores, consideramos que os méritos desta ultrapassam claramente os deméritos quando comparando as duas.

Efectivamente, propõe-se nesta tese uma abordagem que ao contrário da divisão feita por Peltier, que de forma muito linear e restritiva o faz, não divide o universo dos ataques entre ataques humanos e técnicos. De facto, a divisão de Peltier não é mais aplicável numa época em que a fronteira entre estes domínios é ténue, para não dizer inexistente. É hoje uma realidade que para a nova geração o termo "tecnologia" não tem virtualmente significado pois nunca conheceram o mundo sem ela.

Complementarmente, a abordagem proposta potencia a definição e operacionalização de políticas de segurança orientadas às plataformas em que os ataques são realizados, capitalizando

a acumulação e cooperação de tais políticas para a defesa relativamente a ataques que dependem da utilização conjunta, em paralelo ou sequencialmente, de vários tipos de técnicas/plataformas. A classificação taxonómica de Peltier falha sistematicamente neste ponto ao limitar e limitar-se à taxonomia proposta. É impossível negligenciar a crescente desmaterialização de processos e a exponencial integração entre a vida das pessoas e a tecnologia (redes sociais, comunicação com partes terceiras, etc.) implicando tal que ataques antes considerados exclusivamente de base técnica ou base humana poderão ser agora simultaneamente de ambas as naturezas (por exemplo, o *dumpster diving*, antes exclusivamente associado à recolha e inspecção do lixo físico produzido por indivíduos é hoje uma prática digital em que se investiga e analisa a pegada digital desses mesmos indivíduos (informação "deixada" em computador públicos, conteúdo de discos rígidos que são enviados para arranjo, etc.).

Relativamente à definição da espionagem como uma técnica de ataque de engenharia social é importante realçar-se que sendo o objectivo da espionagem a obtenção de informação, este objectivo poderá ser conseguido pela aplicação de um conjunto de outras técnicas. Desta forma pode-se definir a espionagem como o resultado da aplicação de um conjunto de diversas técnicas.

De facto, a natureza não mutuamente exclusiva da taxonomia agora proposta permite considerá-la como passível de evoluções (aumentos, reduções, alterações, etc.) e não uma definição estática restritiva ao espelhamento da própria evolução da tecnologia e de como o homem interage com esta e como a usa para interagir com os outros.

Uma consequência do proposto nesta tese é um possível realinhamento do desenvolvimento das políticas de segurança, desejavelmente mais simples, fragmentadas e orientadas à "defesa de plataformas" de ataque específicas do que à "defesa dos ataques" em si. Efectivamente, no desenvolvimento das políticas de segurança, estas deverão estar orientadas à utilização dos diversos serviços que poderão ser usados como plataformas de ataque. Tomando como exemplo a técnica *Tailgating*, onde o engenheiro social - explorando as diversas falhas humanas - consegue obter o acesso ao local. Num processo com o objetivo de redução do risco na aplicação desta técnica, seria necessária a implementação de um conjunto de mecanismos de controlo eficientes e a consciencialização das pessoas sobre os riscos do não cumprimento das normas de segurança.

É importante referir-se que as preocupações com a segurança não se devem limitar apenas às ameaças concretizadas por entidades externas, dado que os ataques internos também representam uma enorme ameaça à segurança.

A engenharia social, actualmente, é uma preocupação na segurança da informação. Através da formação e da consciencialização da pessoa e da implementação de mecanismos de forma a colmatar as possíveis falhas humanas será possível aumentar o nível de segurança da organização. Para uma boa gestão da segurança é também importante que os responsáveis TI tenham um bom conhecimento das boas práticas de segurança e que sejam capazes de acompanhar a evolução das tecnologias.

No desenvolvimento das políticas de segurança, é necessário que estas sejam simples, compreensíveis e executáveis. As políticas deverão ser testadas no sentido de validar a sua aplicabilidade. As políticas deverão ser desenvolvidas para as pessoas e não contra elas, pois quando não existe a sua compreensão e aceitação não serão cumpridas.

5.2. TRABALHO FUTURO

Considerando o reduzido corpo de conhecimento nesta área, são claramente necessários mais estudos afins a este e aos que este referencia. Consequentemente, sugerem-se as seguintes linhas de investigação:

- investigação futura, semelhante, em que a amostra fosse mais abrangente relativamente à localização geográfica, às habilitações, às profissões e à idade dos utilizadores. Esta investigação permitiria identificar as diferenças no conhecimento e nas atitudes relativas à segurança, inclusivamente de forma comparada com os resultados agora apurados;

- desenvolvimento de uma investigação dirigida aos ataques internos de engenharia social, que tipicamente são depois nomeados como "fraude";

- desenvolvimento de um conjunto de políticas de segurança que permitissem mitigar os riscos de ataque de engenharia social;

- simulação de um ataque de engenharia social a algumas instituições, entre elas, instituições financeiras e organismos públicos. Esta investigação teria como objectivo identificar as vulnerabilidades e validar as políticas de segurança implementadas.

BIBLIOGRAFIA

Abraham, S.; Chengalur-Smith, I.;. (2010). *An overview of social engineering malware: Trends, tactics and implications. .* Technology in Society.

Allan, A., Noakes-Fry, K., & Mogull, R. (2005). *Business Update:How Businesses Can Defend Against Social Engineering Attacks.* Gartner.

Allen, Malcolm. (2007). *Social Engineering: A means to violate a computer system.* SANS Institute.

Baer, M. H. (2008). *Corporate Policing and Corporate Governance: What Can We Learn from Hewlett-Packard´s Pretexting Scandal.* University of Cincinnati Law Review, Corporate Law Symposium.

BARDIN. L. (1977). In *Análise de conteúdo.* Lisboa: Edições 70.

BS ISO/IEC 27002. (2005). *British Standard - Information technology -- Security techniques -- Code of practice for information security management.* ISO (International Organization for Standardization).

Buetler, I. (2009). *Social Engineering Test cases.* From Compass Security AG: http://www.csnc.ch/misc/files/publications/Social_Engineering_V2.0.pdf

Cialdini, R. B. (2001). *Influence: Science and Practice.* USA: Ally & Bancon.

Cohen, L., Manion, L., & Morrison, K. (2007). *Research methods in Education* (6 ed.). Londres: Routledge.

Commer, D. (1998). *Interligação em redes com TCP/IP.* Brazil/Rio de Janeiro : Campus: ARX Publicações.

Corporation, M. (2006). *How to protect insiders from social engineering threats: Midsize business security guidance.* San Francisco: Microsoft Corporation.

Dinis, J. A.;. (2005). *Guerra de Informação - Perspectivas de Segurança e Competitividade.* Sílabo.

Foozy, F. M., Ahmad, R., Abdollah, M. F., Yusof, R., & Zaki, M. (2011). *Generic Taxonomy of Social Engineering Attack.* Malaysian: Malaysian Technical Universities International Conference on Engineering & Technology.

Ghiglione, R., & Matalon, B. (1992). *O Inquérito, Teoria e Prática.* Oeiras: Celta Editora.

Gil, A. C. (1999). *Métodos técnicas de pesquisa social* (5ª ed.). São Paulo: Atlas.

Gil, A. C. (2008). *Métodos e técnicas de pesquisa social* (6 ed.). São Paulo, Brasil: Atlas.

Gonçalves, D. I. (2008). *Pesquisas de marketing pela internet: As percepções sob a óptica dos entrevistados.* Revista de Administração Mackenzie.

Gragg, D. (2002). *A multi-level defense against social engineering.* Washington: SANS Institute.

Granger, S. (2001). *Social Engineering Fundamentals, Part I: Hacker Tactics*. Infocus.

Granger, S. (2002). *Social engineering fundamentals, part II: Combat strategies.* Infocus.

Indrajait, Richardus Eko;. (2012). *Social Engineering Taxonomy The Scream Method.* (F. T. Colloquium, Ed.) SGU.

ISACA. (1998). *Information Systems Audit and Control Association in Cobit Control Objectives.*

Ivaturi, Koteswara; Janczewski, Lech. (2011). *A Taxonomy for Social Engineering attacks.* (I. C. Information, Ed.) Association for Information Systems AIS Electronic Library (AISeL).

Janczewski, L. J.; Lingyan, F. (2010). Social engineering-based attacks: Model and new zealand perspective. *in Computer Science and Information Technology (IMCSIT), Proceedings of the 2010 International Multiconference on.*

Jordán, Gladys Castillo. (2008). *Aula de Métodos Estatisticos: Intervalo de Confiança.* Universidade de Aveiro.

Kee, Jared. (April 2008). *Social Engineering: Manipulating the Source.* SANS Institute.

Lee, D. H., Choi, K. H., & Kim, K. J. (2007). *Intelligence Report and the Analysis Against the Phishing Attack Wich Uses a Social Engineering Technique.* Springer-Verlag.

Long, J. (2008). *No Techo Hacking.* Syngress publishing, Inc.

Maiwald, E. (2003). *Network security: A beginner's guide.* San Francisco: McGraw-Hill Osborne Media.

Mann, I., & L., A. (2006). *Hacking the human: An introduction to social.* Bradford: ECSC.

Markham, A. N. (2004). *Qualitative research: Theory, methods and practice* (2ª ed.). CA: Sage.

Mccartthy, M. p., & Campbell, S. (2003). *Transformação na Segurança Electrónica: Estratégias e gestão da defesa Digital.* Person Education do Brasil.

McDowell, Mindi. (June 2007). *White paper: Avoiding Social Engineering and Phishing Attacks,Cyber Security Tip ST04-014.* Carnegie Mellon University.

Miguel, António. (2002). *Gestão do Risco e da Qualidade no Desenvolvimento de Software.* FCA.

Minayo, M. C. (1994). *Pesquisa Social: teoria, método e criatividade.* Petrópolis: Vozes.

Miranda, R. C. (1999). *Ciência da Informação* (Vols. v.28,n.3). Brasília.

Mitnick, K. D., & W., L. S. (2002). *The art of deception: controlling the human element of security.* Indianapolis: Wiley.

Mitnick, K. D., & W., L. S. (2006). *The art of intrusion: The real stories behind the exploits of hackers, intruders, & deceivers.* Indianapolis: Wiley.

Paisana, M., & Lima, T. (2012). *Sociedade em Rede. A Internet em Portugal 2012.* Obercom.

Pardal, L.; Correia, E. (1995). *Métodos e Ténicas de Investigação Social.* Arial Editores.

Peltier, T. (2006). *Social Engineering: Concepts and Solutions. In: Information Security and Risk Management.* The official journal of (ISC).

Peltier, T.R. (2004). *Social Engineering: Concepts and Solutions. Information Systems Security.* Corporate ResourceNet database.

Quivy, R. C. (1992). *Manual de Investigação em Ciências Sociais.* Lisboa: Gradiva.

Quivy, R., & Campenhoudt, L. (1992). *Manual de Investigação em Ciências Sociais.* Lisboa: Gradiva.

Richardson, R. J. (1999). *Pesquisa Social: Métodos e Técnicas.* São Paulo: Atlas.

Sandouka, H., Cullen, A. J., & Mann, I. (2009). Social Engineering Detection Using Neural Networks. *in CyberWorlds, 2009.*

Scambray, J., McClure, S., & Kurtz, G. (2001). *Hacking Exposed.* McGraw-Hill .

Stevens, G. (2002). *Enhancing defenses against social engineering.* Washington: SANS Institute.

Tiantian, Q. (2007). *An Investigationof Heuristics of Human Judgment in Detecting Deception and Potential Implications in Countering Social Engineering in Intelligence and Security Informatics.* IEEE.

Tuckman, B. W. (2000). *Manual de Investigação em Educação.* Lisboa: Fundação Calouste Gulbenkian.

Twitchell, D. P. (2006). Social Engineering in Information Assurance Curricula. In *in Proceedings of the 3rd annual conference on Information security curriculum development.* (pp. 191-193). Georgia: ACM: Kennesaw.

Workman, M. (2008). *A teste of interventions for security threats from social engineering.* Emerald Group Publishing Limited.

Zager, M. (2002). *Who are the hackers?* Infosec News.

Referências Electrónicas

Lively Jr, C. (2004).

Psychological Based Social Engineering.

SANS Institute

URL: http://www.giac.org/paper/gsec/3547/psychological-based-social-engineering/105780

Retrieved: 23-01-2012

Manjak, M. (2006).

Social Engineering Your Employees to Information Security.

SANS Institute

URL:http://www.sans.org/reading_room/whitepapers/awareness/social-engineering-employees-information-security_1686

Retrieved: 10-11-2011

Reardon, L. (2009).

Email Statistics Report, 2009 - 2013.

From The Radicati Group: A Tecnology Market Research:

URL: http://www.radicati.com/?p=3237

Retrieved: 30-11-2011

Redmon, K. C. (2005).

Mitigation of Social Engineering attacks in Corporate America.

Infosecwirets

URL: http://www.infosecwriters.com/text_resources/pdf/Social_Engineering_KRedmon.pdf

Retrieved: 5-01-2012

Research Dimensional. (2011).

The Risk Of SocialL Engineering on Information Security: A Survey of IT Pprofessionals.

Dimensional Research

URL: http://www.checkpoint.com/press/downloads/social-engineering-survey.pdf

Retrieved: 23-11-2011

Lafrance, Yves (2004).

Psychology: A Precious Security Tool.

SANS Institute.

URL: http://www.sans.org/reading_room/whitepapers/engineering/psychology-precious-security-tool_1409

Retrieved: 23-02-2012

Srivastava, Tushar Vishesh. (2007).

Phishing and Pharming – The Deadly Duo.

SANS Institute

URL: http://www.sans.org/reading_room/whitepapers/privacy/phishing-pharming-evil-twins_1731

Retrieved: 5-12-2011

Haley, Kevin. (2012).

Cinco principais previsões de segurança da Symantec para 2013

Official Blog da Symantec.

URL: http://www.symantec.com/connect/blogs/cinco-principais-previsoes-de-seguranca-da-symantec-para-2013

Retrieved: 29-11-2012

Symantec. (2010).

Symantec MessageLabs Email Security.cloud.

Symanteccloud

URL:http://www.symanteccloud.com%2Fpt%2Fbr%2Fdatasheet%2FDatasheet_Email_Security_cloud_BR.pdf&ei=RRZ6UNGQAqmh0QXkkIHoDQ&usg=AFQjCNFtcYHg3OvfYwC03hRgJPerurGqTw&sig2=zfu4iqRS

Retrieved: 5-10-2011

Thapar, A. (2007).

Social Engineering - An Attack Vector Most Intricate to Tackle.

Infosec Writers

URL: http://www.infosecwriters.com/text_resources/pdf/Social_Engineering_AThapar.pdf

Retrieved: 14-10-2011

US-CERT. (2010)

Technical Information Paper Cyber Threats to Mobile Devices

US-CERT

URL: http://www.us-cert.gov/reading_room/TIP10-105-01.pdf

Retrieved: 15-12-2011

ANEXOS

ANEXO I – INQUÉRITO AOS RESPONSÁVEIS TI

INQUÉRITO ÀS EMPRESAS

1.Localização:

2. Identifique o sector de actividade:

Sector Primário ○
Sector Secundário ○
Sector Terciário ○

3. Identifique o ramo de negócio

Produção ○
Transformação ○
Distribuição ○
Serviços ○
Banca ○
Seguros ○
Telecomunicações ○
Organismos Públicos ○
OUTROS ○

4. Tipologia de Empresa

Constituída por menos de 10 pessoas ○
Constituída entre 10 a 249 pessoas ○
Constituiída por mais de 250 pessoas ○

5. Identifique a sua área formação:

Tecnologias de Informação ○
Outras ○

6. Identifique os serviços que utilizam através :

- Telefone

Serviços ☐
Contacto com os parceiros ☐
Serviços Públicos ☐
Instituições Financeiras ☐
Transacções comerciais ☐

Internet

Utilizam outros serviços ☐
Contacto com os parceiros ☐
Serviços Públicos Online ☐
Homebanking ☐
Transacções Comerciais ☐
Pesquisa de Informação ☐
Utilizam serviços de *Chat* ☐
Fazer/Receber chamadas através da Internet ☐

Redes de partilha de ficheiros - P2P (peer-to-peer) ☐
Realizam Downloads ☐
Utilizam serviços de partilha e armazenamento de ficheiros (ex: dropbox) ☐
Possuem página web ☐
Frequentam Blogues ☐
Frequentam Redes Sociais ☐
Enviam/Recebem emails ☐

7. Identifique os possíveis alvos de ataque de engenharia social

Administradores ☐
Assistentes Executivos ☐
Recursos Humanos ☐
Novos Trabalhadores ☐
Equipa TI ☐

8. Identifique as principais medidas de segurança aplicadas

Realizam cópias de segurança - *Backups* ☐
Possuem políticas de segurança ☐
Utilizam mecanismos de controlo de acesso ☐
Destroem com segurança os documentos ☐
Os códigos de identificação não são óbvios nem identificáveis ☐
Alteram as passwords periodicamente ☐
Definem passwords diferentes para aceder a sites seguros ☐
Não utilizam pen´s externas dentro da Organização ☐
Pedem para o browser memorizar a password ☐
Nunca se deixam enganar por acções de terceiros que utilizam técnicas para obtenção de informação pessoal ☐
Em acessos sensíveis, utilizam passwords com pelo menos 20 caracteres ☐
Nunca abrem ficheiros anexos em email sem ter a certeza de quem é o remetente ☐
Nunca introduzem elementos identificativos ou confidenciais em sites sem confirmar se estão num ambiente seguro ☐
Nunca fornecem os dados pessoais através de email ou qualquer outro meio ☐
Verificam o endereço do site ☐
Têm o software actualizado ☐
Utilizam uma firewall ☐
Têm instalado um antivírus ☐

9. Já ouviram falar em ataques de engenharia social

SIM ○
NÃO ○

10. Assinale os ataques de que já ouviram falar:

- [ ] Shoulder Surfing
- [ ] Social Reverse
- [ ] Malware
- [ ] Pop-up
- [ ] Tailgating
- [ ] Baiting
- [ ] Hoaxing
- [ ] Vishing
- [ ] Spam Mails
- [ ] Smishing
- [ ] Pretexting/Impersonation
- [ ] Phishing
- [ ] Spying and Eavesdropping
- [ ] Pharming
- [ ] Dumpster Diving
- [ ] Interesting Software
- [ ] Footprint

11. Foram vítima de algum tipo de ataque de engenharia social?

- ○ SIM
- ○ NÃO
- ○ NS/NR

12. Identifique o tipo de ataque que foram alvo:

- [ ] Shoulder Surfing
- [ ] Social Reverse
- [ ] Malware
- [ ] Pop-up
- [ ] Tailgating
- [ ] Baiting
- [ ] Hoaxing
- [ ] Vishing
- [ ] Spam Mails
- [ ] Smishing
- [ ] Pretexting/Impersonation
- [ ] Phishing
- [ ] Spying and Eavesdropping
- [ ] Pharming
- [ ] Dumpster Diving
- [ ] Interesting Software
- [ ] Footprint

13. Identifique o principal objectivo do ataque:

Roubo da Informação
Financeiro
Vantagem Competitiva
Vingança
Outro
NS/NR

14. Indique a que entidades participaram o ataque:

Judicial
Fornecedor do Serviço
Provedor de Acesso (ISP)
Outro
NS/NR

15. Indique qual a abordagem de segurança adoptada depois do ataque

Mantiveram a abordagem anterior
Adoptaram uma nova abordagem
NS/NR

16. Promovem acções de formação para os colaboradores?

SIM
NÃO
NS/NR

17. Qual o sentimento em relação aos riscos de segurança no futuro?

Piorar
Melhorar
Manter
NS/NR

18. Identifique no futuro quais serão as plataformas mais utilizadas nos ataques de engenharia social?

Ataque presencial
Telefone
Redes Sociais
Páginas Web
Emails
VoIP
Outro
NS/NR

Obrigado pela sua colaboração

ANEXO II – INQUÉRITO AOS UTILIZADORES

1.Localização:

2. Email:

3. Idade:

4. Sexo:

Feminino ○

Masculino ○

5. Identifique os serviços que utiliza através:

Telefone

Serviços ☐

Instituições Públicas ☐

Instituições Financeiras ☐

Transacções Comerciais ☐

Internet

Outros Serviços ☐

Serviços Públicos Online ☐

Homebanking ☐

Transacções Comerciais ☐

Pesquisa de Informação ☐

Serviços de chat ☐

Fazer/Receber chamadas através da Internet ☐

Realiza Downloads ☐

Serviços de partilha e armazenamento de ficheiros (ex: dropbox) ☐

Redes de partilha de ficheiros - P2P (peer-to-peer) ☐

Partilha conteúdos pessoais ☐

Frequenta blogues ☐

Frequenta redes sociais ☐

Enviam/Recebem emails ☐

6. Quando realiza operações através do telefone/internet preocupa com a segurança:

Telefone

SIM ○

NÃO ○

Internet

SIM ○

NÃO ○

7. Identifique as principais medidas de segurança aplicadas

Têm instalado um antivírus ☐

Utiliza uma firewall ☐

Têm o software actualizado ☐

Verifica o endereço do site ☐

Nunca fornece dados pessoais através de email ou qualquer outro meio	☐
Nunca introduz elementos identificativos ou confidenciais em sites sem confirmar se estão num ambiente seguro	☐
Nunca abre ficheiros anexos ao email sem ter a certeza de quem é o remetente	☐
Em acessos sensíveis, utiliza passwords com pelo menos 20 caracteres	☐
Nunca se deixa enganar por acções de terceiros que utilizam técnicas para obtenção de informação pessoal	☐
Pede para o browser memorizar a password	☐
Não acede nem efectua operações em computadores públicos	☐
Define passwords diferentes para aceder a sites seguros	☐
Não acede aos sites do banco ou outros organismos através de links	
Altera as passwords periodicamente	☐
Os códigos de identificação não são óbvios nem identificáveis	☐
Realiza cópias de segurança -backups	☐
Destrói com segurança os documentos	☐
Não utiliza pen-s pessoais em computadpores públicos	☐
8. Indique a proveniência do software antivírus?	
Adquirido na loja	○
Versão grátis	○
Obtido na internet	○
Cópia de um amigo	○
NS/NR	○
9. Já ouviu falar em ataques de engenharia social	
SIM	○
NÃO	○
10. Assinale as técnicas de que já ouviu falar:	
Malware	☐
Shoulder Surfing	☐
Social Reverse	☐
Pop-up	☐
Tailgating	☐
Baiting	☐
Hoaxing	☐
Vishing	☐
Spam Mails	☐
Smishing	☐
Pretexting/Impersonation	☐
Phishing	☐
Spying and Eavesdropping	☐
Pharming	☐
Dumpster Diving	☐
Interesting Software	☐
Footprint	☐

11. Foi vítima de algum tipo de ataque de engenharia social?

SIM ○
NÃO ○
NS/NR ○

12. O ataque de que foi alvo, foi bem-sucedido?

SIM ○
NÃO ○
NS/NR ○

13. Identifique o tipo de ataque que foram alvo:

Shoulder Surfing ☐
Social Reverse ☐
Malware ☐
Pop-up ☐
Tailgating ☐
Baiting ☐
Hoaxing ☐
Vishing ☐
Spam Mails ☐
Smishing ☐
Pretexting/Impersonation ☐
Phishing ☐
Spying and Eavesdropping ☐
Pharming ☐
Dumpster Diving ☐
Interesting Software ☐
Footprint ☐

14. Identifique o principal objectivo do ataque:

Financeiro ○
Acesso à informação ○
Vingança ○
Vantagem Competitiva ○
Outros ○
NS/NR ○

15. Indique a que entidade participou o ataque:

Judicial ○
Fornecedor do Serviço ○
Provedor do serviço de internet
Outra ○
NS/NR ○

16. Indique qual a plataforma usada na realização do ataque:

VoIP ○
Redes Sociais ○
Páginas Web ○
E-mail ○
Telefone ○
Ataque Presencial ○
Outra ○
NS/NR ○

17. Identifique no futuro quais serão as plataformas de ataque mais utilizadas?

VoIP ○
Redes Sociais ○
Páginas Web ○
Emails ○
Telefone ○
Ataque Presencial ○
Outro ○
NS/NR ○

18. Qual o sentimento em relação aos riscos de segurança no futuro?

Piorar ○
Melhorar ○
Manter ○
NS/NR ○

Obrigado pela sua colaboração

ANEXO III - TABELAS COM OS CÁLCULOS DAS MARGENS DE ERRO

Tabela 1. – Cálculo das margens de erro relativo ao gráfico 3.4

n=41

	Identifique o tipo de serviço que utilizam:	**%**	**Margem de erro**	**é provável os valores estarem compreendidos entre**	
Telefone	Serviços	80%	12%	68%	93%
	Contacto com os parceiros	98%	5%	93%	100%
	Serviços Públicos	39%	15%	24%	54%
	Instituições Financeiras	34%	15%	20%	49%
	Transacções Comerciais	61%	15%	46%	76%
Internet	Utilizam outros serviços	54%	15%	38%	69%
	Contacto com parceiros	49%	15%	33%	64%
	Serviços Públicos Online	93%	8%	85%	100%
	Homebanking	98%	5%	93%	100%
	Transacções Comerciais	44%	15%	29%	59%
	Pesquisa de Informação	98%	5%	93%	100%
	Utilizam Serviços de Chats	54%	15%	38%	69%
	Fazer/Receber Chamadas através da Internet	5%	7%	0%	11%
	Redes de partilha de ficheiros - P2P (Peer-to-peer)	2%	5%	0%	7%
	Realizam Downloads	51%	15%	36%	67%
	Utilizam serviços de partilha e armazenamento de ficheiros, ex: Dropbox	39%	15%	24%	54%
	Possuem página web	34%	15%	20%	49%
	Frequentam Blogues	24%	13%	11%	38%
	Frequentam Redes Socias	20%	12%	7%	32%
	Enviam/Recebem E-mails	100%	0%	100%	100%

Tabela 2 – Cálculo das margens de erro relativo ao gráfico 3.5

n=41

Descrição	%	Margem de erro	é provável os valores estarem compreendidos entre	
Realizam cópias de segurança - backups	45%	15,23%	30%	60%
Possuem políticas de segurança	30%	14,03%	16%	44%
Utilizam mecanismos de controlo de acesso	15%	10,93%	4%	26%
Destroem com segurança os documentos	70%	14,03%	56%	84%
Os códigos de identificação não são óbvios nem identificáveis	57%	15,15%	42%	72%
Alteram as passwords periodicamente	40%	15,00%	25%	55%
Definem passwords diferentes para aceder a sites seguros	35%	14,60%	20%	50%
Não utilizam pen´s externas dentro da Organização.	60%	15,00%	45%	75%
Pedem para o browser memorizar a password	22%	12,68%	9%	35%
Nunca se deixam enganar por acções de terceiros que utilizam técnicas para obtenção de informação pessoal.	44%	15,19%	29%	59%
Em acessos sensíveis, utilizam passwords com pelo menos 20 caracteres	16%	11,22%	5%	27%
Nunca abrem ficheiros anexos em email sem ter a certeza de quem é o remetente.	53%	15,28%	38%	68%
Nunca introduzem elementos identificativos ou confidenciais em sites sem confirmar se estão num ambiente seguro.	59%	15,06%	44%	74%
Nunca fornecem os dados pessoais através de email ou qualquer outro meio.	66%	14,50%	51%	81%
Verificam o endereço do Site	55%	15,23%	40%	70%
Têm o software actualizado	88%	9,95%	78%	98%
Utilizam uma firewall	91%	8,76%	82%	100%
Têm instalado um antivirus	97%	5,22%	92%	100%

Tabela 3 – Cálculo das margens de erro relativo ao gráfico 3.6

n=41

	%	Margem de erro	os valores estão compreendidos entre		Amostra
SIM	88%	10,02%	77,79%	97,82%	36
NÃO	2%	4,7%	-2,28%	7,16%	1
NS/NR	10%	9,1%	0,67%	18,84%	4

Tabela 4 – Cálculo das margens de erro relativo ao gráfico 3.7

n=36

Técnicas	%	Margem de erro	os valores estão compreendidos entre	
Shoulder Surfing	42%	16%	25,55%	58,45%
Social Reverse	25%	14%	10,57%	39,43%
Malware	92%	9%	82,96%	100,00%
Pop-up	69%	15%	53,58%	84,42%
Tailgating	33%	16%	17,33%	48,67%
Baiting	44%	17%	27,45%	60,55%
Hoaxing	36%	16%	20,00%	52,00%
Vishing	31%	15%	15,58%	46,42%
Spam Mails	92%	9%	82,96%	100,00%
Smishing	16%	12%	3,78%	28,22%
Pretexting/Impersonation	44%	17%	27,45%	60,55%
Phishing	86%	12%	74,43%	97,57%
Spying and Eavesdropping	47%	17%	30,36%	63,64%
Pharming	28%	15%	13,03%	42,97%
Dumpster Diving	44%	17%	27,45%	60,55%
Interesting Software	42%	16%	25,55%	58,45%
Footprint	28%	15%	13,03%	42,97%

Tabela 5 – Cálculo das margens de erro relativo ao gráfico 3.8

n=36

	%	Margem de Erro	os valores estão compreendidos entre	
SIM	83%	12%	71,16%	95,51%
NÃO	6%	7%	0%	13,04%
NS/NR	11%	10%	0,84%	21,38%

Tabela 6 – Cálculo das margens de erro relativo ao gráfico 3.9

n=30

Técnicas	%	Margem de erro	os valores estão compreendidos entre	
Shoulder Surfing	3%	6%	0%	9,76%
Social Reverse	3%	6%	0%	9,76%
Malware	77%	15%	61,53%	91,80%
Pop-up	33%	17%	16,46%	50,20%
Tailgating	7%	9%	0%	15,59%
Baiting	7%	9%	0%	15,59%
Hoaxing	17%	13%	3,33%	30,00%
Vishing	10%	11%	0%	20,74%
Spam Mails	90%	11%	79,26%	100,00%
Smishing	13%	12%	1,17%	25,50%
Pretexting/Impersonation	30%	16%	13,60%	46,40%
Phishing	67%	17%	49,80%	83,54%
Spying and Eavesdropping	17%	13%	3,33%	30,00%
Pharming	3%	6%	0%	9,76%
Dumpster Diving	10%	11%	0%	20,74%
Interesting Software	13%	12%	1,17%	25,50%
Footprint	3%	6%	0%	9,76%

Tabela 7 – Cálculo das margens de erro relativo ao gráfico 3.10

n=41

	Amostra	%	Margem erro	Os valores estão compreendidos entre	
Equipa TI	2	5%	6,59%	0%	11,47%
Novos Trabalhadores	18	44%	15,19%	28,71%	59,09%
Recursos Humanos	6	15%	10,82%	3,82%	25,45%
Assistentes Executivos	11	27%	13,56%	13,27%	40,39%
Administradores	4	10%	9,08%	0,67%	18,84%

Tabela 8 – Cálculo das margens de erro relativo ao gráfico 3.11

n=30

	%	Margem Erro	os valores estão compreendidos entre	
Roubo da Informação	53%	18%	35,48%	71,19%
Financeiro	23%	15%	8,20%	38,47%
Vantagem Competitiva	7%	9%	0%	15,59%
Vingança	13%	12%	1,17%	25,50%
Outro	3%	6%	0%	9,76%

Tabela 9 – Cálculo das margens de erro relativo ao gráfico 3.12

n=30

	%	Margem de erro	os valores estão compreendidos entre		Amostra
Judicial	27%	16%	10,84%	42,49%	8
Fornecedor do Serviço	20%	14%	5,69%	34,31%	6
Provedor de Acesso (ISP)	10%	11%	0%	20,74%	3
Outro	7%	9%	0%	15,59%	2
NS/NR	37%	17%	19,42%	53,91%	11

Tabela 10 – Cálculo das margens de erro relativo ao gráfico 3.13

n=30

	%	Margem de Erro	os valores estão compreendidos entre	
Mantiveram a abordagem anterior	33%	17%	16,46%	50,20%
Adoptaram uma nova abordagem	20%	14%	5,69%	34,31%
NS/NR	47%	18%	28,81%	64,52%

Tabela 11 – Cálculo das margens de erro relativo ao gráfico 3.14

n=30

	%	Margem de Erro	os valores estão compreendidos entre	
SIM	23%	15%	8,20%	38,47%
NÃO	40%	18%	22,47%	57,53%
NS/NR	37%	17%	19,42%	53,91%

Tabela 12 – Cálculo das margens de erro relativo ao gráfico 3.15

n=30

	%	Margem Erro	os valores estão compreendidos entre	
Piorar	60%	18%	42,11%	77,89%
Melhorar	3%	7%	0%	9,89%
Manter	27%	16%	10,52%	42,81%
NS/NR	10%	11%	-0,95%	20,95%

Tabela 13 – Cálculo das margens de erro relativo ao gráfico 3.16

n=30

	%	Margem de erro	os valores estão compreendidos entre	
Ataque Presencial	3%	6%	0%	9,76%
Telefone	3%	6%	0%	9,76%
Redes Socias	40%	18%	22,47%	57,53%
Web page	13%	12%	1,17%	25,50%
Emails	27%	16%	10,84%	42,49%
VoiP	7%	9%	0%	15,59%
Outro	3%	6%	0%	9,76%
NS/NR	3%	6%	0%	9,76%

Tabela 14 – Cálculo das margens de erro relativo ao gráfico 3.19

n=393

	%	Margem de Erro	os valores estão compreendidos entre		Indicaram o email	Amostra
Masculino	42%	9%	33,16%	50,31%	53	127
Feminino	71%	8%	63,16%	78,94%	189	266

Tabela 15 – Cálculo das margens de erro relativo ao gráfico 3.20

n=393

	%	Margem de erro	os valores estão compreendidos entre		Indicaram o email	Amostra
22 a 34 anos	42%	8%	34,70%	50,11%	67	158
35 a 49 anos	51%	7%	44,15%	58,55%	95	185
mais 50 anos	60%	14%	46,42%	73,58%	30	50

Tabela 16 – Cálculo das margens de erro relativo ao gráfico 3.21

	Identifique o tipo de serviço que utilizam:	Total	Margem de erro	é provável os valores estarem compreendidos entre	
Telefone	Serviços	**41%**	5%	36%	46%
	Instituições Públicas	**34%**	5%	29%	39%
	Instituições Financeiras	**38%**	5%	33%	43%
	Transacções Comerciais	**44%**	5%	39%	49%
Internet	Outros serviços	**37%**	5%	32%	42%
	Serviços Públicos Online	**55%**	5%	50%	60%
	Homebanking	**56%**	5%	51%	61%
	Transacções Comerciais	**48%**	5%	43%	53%
	Pesquisa de Informação	**98%**	1%	97%	99%
	Serviços de Chats	**64%**	5%	59%	68%
	Fazer/Receber Chamadas através da Internet	**20%**	4%	16%	24%
	Realiza Downloads	**66%**	5%	61%	71%
	Serviços de partilha e armazenamento de ficheiros, ex: Dropbox	**25%**	4%	21%	30%
	Redes Partilha de ficheiros - P2P (peer-to-peer)	**38%**	5%	33%	43%
	Partilha Conteúdos Pessoais	**31%**	5%	26%	35%
	Frequenta Blogues	**51%**	5%	46%	56%
	Frequenta Redes Socias	**100%**	0%	100%	100%
	Envia/Recebe E-mails	**100%**	0%	100%	100%

Tabela 17 – Cálculo das margens de erro relativo ao gráfico 3.22

n=393

	%	Margem de Erro	os valores estão compreendidos entre		Amostra
Internet	97%	2%	94,52%	98,72%	293
Telefone	63%	10%	53,34%	72,66%	100

Tabela 18 – Cálculo das margens de erro relativo ao gráfico 3.23

n=158	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M13	M14	M15	M16	M17	M18
22 aos 34 anos	96%	87%	86%	69%	73%	66%	68%	45%	51%	44%	61%	58%	67%	55%	66%	26%	37%	52%
Margem de erro	3%	5%	5%	7%	6%	7%	7%	7%	7%	7%	7%	7%	7%	7%	7%	6%	7%	7%
os valores estão compreendidos entre	93%	82%	81%	62%	67%	60%	61%	37%	44%	36%	54%	51%	61%	48%	59%	20%	30%	45%
	99%	92%	91%	76%	80%	73%	74%	52%	59%	51%	68%	65%	74%	62%	73%	32%	44%	59%

n=185	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M13	M14	M15	M16	M17	M18
35 aos 49 anos	92%	81%	79%	62%	66%	52%	52%	38%	62%	52%	60%	40%	58%	41%	42%	15%	30%	43%
Margem de erro	8%	11%	11%	13%	13%	14%	14%	13%	13%	14%	14%	14%	14%	14%	14%	10%	13%	14%
os valores estão compreendidos entre	84%	70%	68%	49%	53%	38%	38%	25%	49%	38%	46%	26%	44%	27%	28%	5%	17%	29%
	100%	92%	90%	75%	79%	66%	66%	51%	75%	66%	74%	54%	72%	55%	56%	25%	43%	57%

N=50	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M13	M14	M15	M16	M17	M18
mais de 50 anos	96%	83%	88%	65%	64%	63%	60%	56%	53%	65%	46%	47%	46%	47%	51%	23%	20%	38%
Margem de erro	3%	6%	5%	7%	7%	8%	8%	8%	8%	7%	8%	8%	8%	8%	8%	7%	6%	8%
os valores estão compreendidos entre	92%	78%	83%	57%	57%	55%	52%	49%	45%	58%	39%	39%	39%	39%	44%	16%	14%	30%
	99%	89%	93%	72%	72%	70%	68%	64%	61%	73%	54%	55%	54%	55%	59%	30%	26%	46%

Tabela 19 – Cálculo das margens de erro relativo ao gráfico 3.24

n=393

	%	Margem de erro	os valores estão compreendidos entre	
Adquirido na loja	23%	4%	18,42%	26,87%
Versão grátis	46%	5%	40,78%	50,83%
Obtido na internet	21%	4%	16,53%	24,69%
Cópia de um amigo	10%	3%	7,35%	13,52%
NS/NR	1%	1%	0%	1,23%

Tabela 20 – Cálculo das margens de erro relativo ao gráfico 3.25

n=393

	%	Margem de Erro	os valores estão compreendidos entre		Amostra
SIM	55%	5%	49,69%	59,73%	215
NÃO	45%	5%	39,52%	49,54%	175

Tabela 21 – Cálculo das margens de erro relativo ao gráfico 3.26

	Malware	Shoulder Surfing	Social Reverse	Popups	Tailgating	Baiting	Hoaxing	Vishing	Spam Mails	Smishing	Pretexting /Impersonation	Phishing	Spying and Eavesdropping	Pharming	Dumpster Diving	Interesting Software	Footprint
22 aos 34 anos	57%	17%	2%	48%	1%	0%	10%	8%	83%	12%	9%	89%	20%	17%	13%	12%	18%
35 aos 49 anos	62%	21%	3%	45%	1%	1%	14%	8%	90%	12%	11%	91%	13%	18%	13%	16%	18%
mais de 50 anos	23%	13%	0%	17%	0%	0%	7%	6%	71%	3%	3%	73%	9%	6%	9%	9%	14%

	CÁLCULO DA MARGEM DE ERRO																
	Malware	Shoulder Surfing	Social Reverse	Popups	Tailgating	Baiting	Hoaxing	Vishing	Spam Mails	Smishing	Pretexting/Impersonation	Phishing	Spying and Eavesdropping	Pharming	Dumpster Diving	Interesting Software	Footprint
22 aos 34 anos	11%	8%	3%	11%	2%	0%	6%	6%	8%	7%	6%	7%	9%	8%	7%	7%	8%
35 aos 49 anos	10%	8%	3%	10%	2%	2%	7%	5%	6%	7%	6%	6%	7%	8%	7%	7%	8%
mais de 50 anos	14%	11%	0%	13%	0%	0%	9%	8%	15%	6%	6%	15%	10%	8%	10%	10%	12%

Tabela 22 – Cálculo das margens de erro relativo ao gráfico 3.27

n=215

	%	Margem de Erro	os valores estão compreendidos entre		Amostra
SIM	40%	7%	33,77%	47,16%	87
NÃO	22%	6%	16,22%	27,50%	47
NS/NR	38%	7%	31,06%	44,28%	81

Tabela 23 – Cálculo das margens de erro relativo ao gráfico 3.28

n=87

	%	Margem de Erro	os valores estão compreendidos entre		Amostra
SIM	17%	8%	9,14%	25,34%	15
NÃO	46%	11%	35,29%	56,66%	40
NS/NR	37%	10%	26,44%	47,12%	32

Tabela 24 – Cálculo das margens de erro relativo ao gráfico 3.29

n=87

Técnicas de Ataque	%	Margem de erro	os valores estão entre	
Shoulder Surfing	0%	0%	0%	0%
Social Reverse	0%	0%	0%	0%
Malware	7%	5%	2%	12%
Pop-up	6%	5%	1%	11%
Tailgating	0%	0%	0%	0%
Baiting	0%	0%	0%	0%
Hoaxing	9%	6%	3%	15%
Vishing	0%	0%	0%	0%
Spam Mails	76%	9%	67%	85%
Smishing	3%	4%	0%	7%
Pretexting/Impersonation	3%	4%	0%	7%
Phishing	53%	10%	42%	63%
Spying and Eavesdropping	3%	4%	0%	7%
Pharming	2%	3%	0%	5%
Dumpster Diving	0%	0%	0%	0%
Interesting Software	5%	4%	0%	9%
Footprint	2%	3%	0%	5%

Tabela 25 – Cálculo das margens de erro relativo ao gráfico 3.30

n=87

	%	Margem de Erro	os valores estão compreendidos entre		Amostra
Financeiro	30%	10%	20,27%	39,50%	26
Acesso a informação	52%	11%	41,22%	62,22%	45
Vingança	9%	6%	3,12%	15,27%	8
Vantagem Competitiva	3%	4%	0%	7,28%	3
Outros	2%	3%	0%	5,45%	2
NS/NR	3%	4%	0%	7,28%	3

Tabela 26 – Cálculo das margens de erro relativo ao gráfico 3.31

n=87

	%	Margem de Erro	os valores estão compreendidos entre		Amostra
Judicial	20%	8%	11,21%	27,87%	17
Fornecedor do Serviço	36%	10%	25,57%	45,70%	31
Provedor do Serviço de Internet	13%	7%	5,66%	19,63%	11
OUTRA	6%	5%	0,86%	10,64%	5
NS/NR	26%	9%	17,17%	35,70%	23

Tabela 27 – Cálculo das margens de erro relativo ao gráfico 3.32

n=87

	%	Margem de Erro	os valores estão compreendidos entre		Amostra
VoIP	5%	4%	0,20%	9,00%	4
Redes Sociais	15%	7%	7,45%	22,43%	13
Páginas Web	22%	9%	13,16%	30,52%	19
E-mails	45%	10%	34,38%	55,28%	39
Telefone	8%	6%	2,33%	13,76%	7
Ataque Presencial	3%	4%	-0,39%	7,28%	3
OUTRA	1%	2%	-1,09%	3,39%	1
NS/NR	1%	2%	-1,09%	3,39%	1

Tabela 28 – Cálculo das margens de erro relativo ao gráfico 3.33

n=87

	%	**Margem de Erro**	**os valores estão compreendidos entre**		**Amostra**
VoIP	5%	4%	0,20%	9,00%	4
Redes Sociais	15%	7%	7,45%	22,43%	13
Páginas Web	22%	9%	13,16%	30,52%	19
E-mails	45%	10%	34,38%	55,28%	39
Telefone	8%	6%	2,33%	13,76%	7
Ataque Presencial	3%	4%	0%	7,28%	3
OUTRA	1%	2%	0%	3,39%	1
NS/NR	1%	2%	0%	3,39%	1

Tabela 29 – Cálculo das margens de erro relativo ao gráfico 3.34

n=393

	%	Margem Erro	os valores estão compreendidos entre		Amostra
Melhorar	5%	2%	2,47%	6,69%	18
Manter	12%	3%	8,69%	15,23%	47
Piorar	52%	5%	47,12%	57,20%	205
NS/NR	31%	5%	26,62%	35,98%	123